National Data Sharing Agreement (DSA)

between

The National Police Chiefs' Council (NPCC)

On behalf of each of the Police Forces listed in Appendix A of this DSA

and

The Solicitors Regulation Authority (SRA)

to provide a framework for the lawful flow and use of information between the SRA and NPCC forces

18 December 2025

Version v1.0

Summary Sheet

Title of DSA:	DSA between the NPCC and the SRA
Purpose of sharing under the DSA:	The SRA mission is to drive confidence and trust in legal services. Sharing under this DSA enables the SRA to assess risk to the public (such as address safeguarding concerns, minimise the risk of financial default, minimise the risk of fraud or other criminality, and identify the risk of financial failure), which supports wider policing purposes.
Lead Signatory (Police):	CC Gavin Stephens, NPCC Chair
Lead Signatory (SRA):	Andrew Turton, Director of Risk and Information Governance
Parties to this DSA:	The Chief Officers of the Police Forces ('Police Force Parties') listed in Appendix A, represented by the NPCC of 50 Broadway, London SW1H 0BL and Solicitors Regulation Authority of the Cube, 199 Wharfside Street, Birmingham B1 1RN
Date DSA comes into force:	18 December 2025
Date for Review of DSA:	3 years after DSA comes into force
DSA Authors:	NPCC DPO, NPFDU DP Manager and SRA
Stakeholders Consulted:	N/A
Data Protection Impact Assessment:	N/A
Disclosure:	This document contains no sensitive information and therefore is suitable for disclosure into the public domain

Version Control

Version No.	Revision Date	Amended by	Summary of Changes
0.1	November 2024	SRA/NPFDU	Initial Draft
1.0	December 2025	SRA/NPFDU	Signed by both parties

Contents

1. Introduction

1.1. This Data Sharing Agreement (DSA) has been developed by the NPCC on behalf of each of the Police Forces listed in Appendix A and the Solicitors Regulation Authority hereafter termed 'Parties' to help facilitate data sharing between those Parties for the purposes set out under Section 2.

1.2. The intention is that this national DSA eliminates the need for each of the represented Police Forces to create their own individual DSA with the other party/parties for this sharing initiative.

1.3. Appendix B sets out the defined terms used in this DSA. These are capitalised within the DSA.

Lead Signatories

1.4. The Parties have identified their respective Lead Signatories. These individuals are their strategic business leads who have confirmed the necessity of data sharing under this initiative.

- The NPCC's Lead Signatory for this data sharing initiative is Gavin Stephens, NPCC Chair.
- The SRA's Lead Signatory for this data sharing initiative is Andew Turton, Director of Risk and Information Governance.

1.5. The DSA contains a signatory section at Section 15 confirming the Parties acknowledge and accept the requirements placed upon them by this DSA.

Data Sharing Leads

1.6. Prior to the commencement of data sharing each of the Police Forces Parties and the Solicitors Regulation Authority will identify a Data Sharing Lead(s) to oversee or develop and maintain the practical arrangements for data sharing under this DSA. More detail can be found in section 5 of this DSA.

Sharing

1.7. The Parties agree that for the purposes of this DSA the term 'sharing' data means providing or disclosing data including personal data to another Party by any means and/or the receiving or collection of data including personal data from another Party by any means.

1.8. In some instances all the Parties may share data with one another; in some cases a single Party may share data with one other Party, but not share data with any other Parties or Party. Signing up to the DSA does not oblige any Party to share data.

Controllership

1.9. Under this initiative data sharing between the Parties is considered to be on a Controller-to-Controller basis.

1.10. The Chief Constables/Commissioners of each Police Force Party listed in Appendix A is regarded as a separate Controller.

1.11. The Solicitors Regulation Authority is regarded as a separate Controller.

2. Why the Parties have agreed to share data (the purpose)

NPCC representing Police Force Parties

2.1. The NPCC has identified the following specific purpose(s) for sharing data under this DSA, where sharing is necessary to achieve these purposes:

Law Enforcement Purposes

2.2. For the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

General Purposes

2.3. For any Common Law Policing Purpose falling outside the specific scope of Law Enforcement Purposes, including assisting the Solicitors Regulation Authority undertaking its statutory and other legitimate services.

The Solicitors Regulation Authority

2.4. The Solicitors Regulation Authority has identified the following specific purpose(s) for sharing data under this DSA:

General Purposes

2.5. To enable the SRA to undertake its regulatory functions, including the assessment of risk to the public such as to:

A. (i) address safeguarding concerns

(ii) minimise the risk of financial default

(iii) minimise the risk of fraud or other criminality; and

(iv) identify the risk of financial failure

B. So that safeguarding concerns, alleged criminality, misconduct, breaches of the SRA's Standards and Regulations or other issues are properly investigated and decided upon;

C. To enable the proper processing of claims or applications for redress or compensation of any description; and

D. For the purposes of investigation, regulatory, disciplinary or other legal (including criminal) proceedings, whether in public or not, provided that the recipient is reasonably considered able to take proper action upon the information.

2.8 Proper purposes may also include further lawful disclosure of the information such as to persons under investigation, witnesses, legal advisors, other regulators, professional bodies, prosecuting bodies and law enforcement agencies including HM Revenue and Customs and the National Crime Agency (or any body which in the future carries out the functions of such bodies).

Illustrative Sharing Scenarios

2.6. Appendix C not used in this DSA.

3. How the sharing can be legally justified

3.1. The Parties agree that the lawful bases for sharing by the NPCC and the SRA respectively are as set out in Appendix D and Appendix E.

3.2. The Parties agree that Appendix D and Appendix E may be updated from time to time as is necessary without the requirement to update the remaining parts of this DSA.

4. Data Protection Compliance

4.1. The Parties agree that the data sharing under this DSA will involve processing of personal data which must be carried out in accordance with Data Protection Legislation.

4.2. The Parties recognise that dependent on their status and the purpose of the processing that some sharing may be for Law Enforcement Purposes while some may be for General Purposes.

4.3. The Parties accept that in terms of Data Protection Legislation they are individual Controllers in their own right in relation to the Personal Data held by them under this DSA until the point where that data is shared directly with and received by another Party – at that point the recipient Party will assume Controllership of their copy of the Personal Data disclosed to them.

4.4. The Parties recognise that the purposes for sharing Personal Data will be specified and made explicit in their privacy policies or data protection policies and their privacy notices (or fair processing notices or data protection notices). They agree to meet any related requirements arising from the Data Protection Legislation.

4.5. The Parties accept that they will never use any Personal Data shared for a purpose that conflicts with or is not compatible with the purpose(s) for which it was shared unless the law allows that to occur.

4.6. The Parties agree to share Personal Data only where it is lawful and fair to do so, subject to exemptions, and where necessary conditions for the processing have been met.

4.7. The Parties recognise individuals whose Personal Data is shared have a series of rights under the Data Protection Legislation and that these will be facilitated.

4.8. The Parties accept the requirements under Data Protection Legislation to maintain respective records of processing activities (RoPA) and agree that this DSA shall be included in such records.

4.9. The Parties will maintain records of sharing requests under this DSA and recognise the importance of keeping such records.

4.10. The Parties assert that they have considered their obligations arising from the Data Protection Legislation and determined that in principle their sharing of Personal Data under this DSA is in compliance with Data Protection Legislation.

4.11. The Parties accept that it is their responsibility individually, or jointly in cases where they act as Joint Controllers, to ensure that on a case-by-case basis sharing of Personal Data under this DSA and its subsequent use by them is in compliance with Data Protection Legislation.

5. The Data Sharing Process

5.1. For Police Forces requesting information from the SRA:

- The SRA operates an Intelligence Unit whose role includes the lawful facilitation of intelligence and information sharing with other bodies.

- The Intelligence Unit assesses information sharing requests on a case-by-case basis. Where lawful and in the public interest, the SRA may provide relevant information to Police Forces on request.
- For access beyond the remit of the Intelligence Unit, Police Forces may seek a Production Order from the court to examine any client file held by the SRA under the provisions of the Police and Criminal Evidence Act 1984 or other statutory authority. Such orders do not override material or information protected by legal professional privilege.
- In all cases, any request for information must be sent in writing to the SRA Intelligence Unit (intel@sra.org.uk). The Single Point of Contact (SPOC) is Christopher Hall, Intelligence Manager. All requests will be recorded and acknowledged within 2 days or as soon as reasonably practicable. The SRA will process, and where lawful and in the public interest, provide the information within 7 days or as soon as reasonably practicable. If for any reason it is unable to do this, it will provide an update after 7 working days and an explanation as to either why the information requested cannot be provided or an estimate as to when the request for information will be processed and the information provided by.

5.2. For the SRA requesting information from Police Forces:

- Most requests for information will be sent to the relevant Police Force Party listed at Annex A by the Intelligence Unit, although some requests will come from other departments within the SRA.
- The Police Force asked to share information will record the request and acknowledge it within 2 days or as soon as reasonably practicable. The Police Force will process, and where lawful and in the public interest, provide the information within 7 working days or as soon as reasonably practicable. If for any reason it is unable to do this, it will provide an update after 7 working days and an explanation as to either why the information requested cannot be provided or an estimate as to when the request for information will be processed and the information provided by.

5.3. Either party may, where it is lawful and in the public interest, choose to share information with the other party on a proactive basis where it believes the information should be so shared. This is subject to the same provisions as above.

6. Relevant Data

6.1. The Parties agree to share, where lawful to do so, relevant and proportionate data necessary for the purpose of the sharing. They agree to ensure individuals involved in the sharing are appropriately trained to make data-sharing decisions to meet this requirement.

7. Data Quality

7.1. The Parties acknowledge that they have a general duty to ensure that Personal Data is accurate, separate to the requirement to take steps where an individual exercises the right to rectification.

7.2. The Parties therefore agree:

- To have systems in place to identify any Personal Data that is inaccurate as to any matter of fact.

- If any Party discovers that Personal Data is inaccurate as to any matter of fact, that Party will ensure that the data is made accurate. They will notify any other Party or Parties with whom they had/have shared that Personal Data of the inaccuracy of the data originally shared and how the data should be corrected/amended.
- If any Party is notified that inaccurate Personal Data has been shared with them, they will immediately take steps to amend the inaccurate data.
- That opinions/allegations that are accurately recorded, even if subsequently found to be untrue, are to be regarded as accurate from a Data Protection perspective. If any Party discovers or is notified that an opinion is incorrect/inaccurate (for example because it is based on inaccurate data), then they will record that the opinion is incorrect/inaccurate. It may still be important to retain the incorrect/inaccurate opinion rather than delete it (for example, to explain why they took specific steps or in case of a complaint or a legal claim). This will need to be judged on a case-by-case basis.
- If any Party discovers that they have shared an opinion which is incorrect/inaccurate because it is based on inaccurate Personal Data , they will notify any Parties within whom they had/have shared the incorrect/inaccurate opinion.

8. How shared data may be used

8.1. The Parties agree that any data shared under the processes described in this DSA will be used or handled in accordance with the terms set out in this DSA.

8.2. Additionally, the shared data may be used by the recipient Party for other appropriate purposes beyond the scope of this DSA where it is compatible with the purpose for which the data was obtained and where it is lawful to do so.

8.3. Where required, the Providing Party will advise where a temporary or permanent restriction on further processing or disclosure is needed. Consideration can also be given to informing the Providing Party of any intention of further processing or disclosure where a restriction had not been notified at the time the data was initially shared.

9. Information Security

9.1. The Parties agree to put in place appropriate physical, technical and organisational measures to protect any data provided to them under this DSA.

9.2. The Parties accept the requirement to ensure that any personnel are able to access only the shared Personal Data necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to Personal Data and Data Protection Legislation.

9.3. The Parties agree to maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.

9.4. The Parties agree to protect the physical security of the shared data. This means they will, as a minimum:

- Ensure their organisation controls physical access to its premises

- Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises
- Ensure proper physical control of printers and photocopiers so that Personal Data is not left lying on printers/photocopiers
- Ensure secure disposal of printed materials, so that materials intended for disposal do not remain accessible. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises
- Ensure that old computers, printers and other electronic equipment are disposed of safely and that all Personal Data is irretrievably deleted from any memory before disposal

9.5. The Parties agree to protect the electronic security of the shared data. This means they will, as a minimum:

- Ensure their organisation has a strong password policy that is adhered to by all personnel. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members
- Ensure their organisation installs security patches on electronic devices (including ensuring all operating systems' updates are installed in line with best practice)
- Ensure personnel are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work
- Ensure that any Wi-Fi connections are secure and that any guest Wi-Fi is on a segregated system, so that guests cannot access other systems from that Wi-Fi
- Ensure that any data that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice
- Ensure that their organisation complies with the best practice of cyber security such as that detailed by the National Cyber Security Centre

9.6. The Parties shall e-mail Special Category Data or information about individuals' criminal convictions or offences, suspected or otherwise, as far as is practical via secure e-mail (e.g. using CJSM); or via email using password protection, with passwords and the data provided in separate emails.

9.7. The Parties agree to have contracts and systems in place to ensure that any contractors or subcontractors managing any aspect of information security or processing Personal Data as a processor on behalf of a Party, are fully aware of and abide by the security requirements set out in this DSA.

9.8. The Parties agree to have robust data breach reporting policies in place, and adhere to them, so that all Personal Data Breaches are reported immediately to personnel responsible for managing Personal Data Breaches when such breaches become apparent. Further, all Parties accept that:

- A "Personal Data Breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data which has been transmitted or stored or processed.

- If it is established that a Data Breach has occurred involving shared data, the Party making the discovery shall inform in writing any Party which is subject to or affected by the Data Breach of the details within a reasonable timescale, 24 hours where possible.
- Following this, any Party who has suffered a Data Breach shall: investigate the cause of the Data Breach and establish the impact; where appropriate, take any necessary action in accordance with its legal responsibilities; and take appropriate steps to mitigate the cause and avoid any repetition.
- The Providing Party will also assess any potential implications for the Data Subject whose information has been compromised and if necessary: notify the Data Subject concerned; inform the Data Subject of their statutory rights; and provide the Data Subject with the appropriate support.
- Where a Data Breach has occurred the Party which is the subject of the Data Breach, supported by any other Party as necessary, must also notify the Information Commissioner's Office within 72 hours unless the Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subject(s). It is the responsibility of the Party managing an incident to investigate and report as appropriate to any other necessary bodies, e.g. Police, Charity Commission etc.
- Personal Data Breaches that reach the threshold for reporting to the Information Commissioner's Office should trigger an exceptional review of this DSA to determine whether changes are required to mitigate any enduring risks arising from the data breach.

10. International Transfers

10.1. The Parties agree that Personal Data may only be transferred between the UK and EU/EEA countries or where an adequacy arrangement has been entered into for that territory. No transfer is allowed to the territories not covered by an adequacy arrangement (such as the United States of America) unless specific and adequate protections are in place (such as Standard Contractual Clauses or the Information Commissioner's International Data Transfer Agreement).

11. Retention

11.1. Parties accept that they must only store shared data in a form that identifies individuals for as long as is necessary for the purposes for which they are processing the Personal Data.

11.2. The Parties also agree that they must each have and implement comprehensive retention schedules, which set out the minimum necessary period of storage for different categories of Personal Data, which are determined taking into account:

- The types of Personal Data processed (organised, for example, by function);
- The purposes for processing the Personal Data;
- Why each type of Personal Data should be retained;
- Any relevant industry standards or guidance;
- Any relevant legal obligations to retain Personal Data for specific periods of time.

11.3. The Parties agree to have systems in place to adhere to the periods in their retention schedules and to review their retention schedules regularly. They will train their personnel so that they are empowered to comply with their retention schedules.

11.4. The Parties agree that where a Party is disbanded or otherwise dissolved the Parties will ensure that the shared Personal Data held by it is disposed of securely and confidentially. Alternatively, where the Party is replaced by a successor organisation, it will ensure that the Personal Data held by it is properly transferred to its successor organisation, subject to the successor organisation becoming a signatory to this DSA. If the successor does not wish to become a signatory to this DSA, the Personal Data will be disposed of securely and confidentially.

12. Subject Rights

The Parties agree that:

12.1. Data Subjects have rights in respect of their Personal Data, and where relevant all parties to this DSA must comply. Where a Party is the recipient of a Subject Rights Application it is that Party's responsibility to lawfully comply with that request in accordance with the Data Protection Legislation and the terms of this DSA.

12.2. Parties will ensure that they have effective procedures for dealing with Subject Rights Applications and complaints from individuals in relation to the use and disclosure of Personal Data. All Parties who are party to this DSA must provide cooperation and assistance to each other in order to resolve any Subject Rights Application or complaint involving shared data.

12.3. Parties may be unaware of the harm that could arise from the disclosure of Personal Data originally obtained from another Party sought via a Data Protection right of access request e.g. prejudice to an ongoing police or safeguarding investigation or harm to the health of the data subject or another person. Consequently, in order to understand the sensitivity of such data the recipient Party will notify the Providing Party as soon as possible, and in any case prior to the disclosure of the data. This will allow the potential implications of responding to the request to be fully assessed and acted upon.

12.4. The same approach will be adopted for Freedom of Information Act requests received by the Police and any other Party which falls under the scope of that act.

13. Training & Advice

The Parties agree:

13.1. To provide all those involved with sharing data under this DSA with sufficient training and guidance to enable them to comply with this DSA. This may include the creation of operational instructions and a Party-specific decision-making model to assist sharing decisions.

13.2. If individuals are uncertain as to what Personal Data can or cannot be shared under this DSA, then they will escalate the query to their line management or in exceptional circumstances to their Data Protection Officer or equivalent individual in their organisation.

14. Administration of the DSA

The Parties agree:

14.1. That this DSA will come into effect on the date stated in the Summary Sheet on page 2 of this DSA.

14.2. That they may withdraw from the DSA upon giving 30 days' written notice to the two Lead Signatories who will cascade notice of that withdrawal to the remaining Parties. A Party who withdraws must continue to comply with the relevant terms of this DSA in respect of any data that the Party has obtained under those terms.

14.3. That the Lead Signatories will together review the DSA no more than twelve months after its implementation. The review will consider whether the DSA is still useful and fit for purpose, identify any emerging issues, and determine whether the DSA should be extended for a further period or whether to terminate it. The decision of the Lead Signatories to extend or terminate the DSA, and the reasons, will be recorded. In the event of a decision to terminate all Parties will be advised of this by the Lead Signatories with the termination to take effect one month after notice is issued.

14.4. That this DSA will be made available unredacted to the public in compliance with the Freedom of Information Act 2000 in its entirety

15. Signatories to this Data Sharing Agreement

15.1. CC Gavin Stephens, as NPCC Chair, has acknowledged and accepted in writing, on behalf of Chief Officers of the Police Forces listed in Appendix A, the requirements placed upon them and others within their organisations by this DSA.

Signature:	
Name:	Gavin Stephens
Position:	NPCC Chair
Date:	4 December 2025

15.2. Andrew Turton has acknowledged and accepted in writing on behalf of the SRA the requirements placed upon him and others within the SRA by this DSA.

Signature:	
Name:	Andrew Turton
Position:	Director of Risk and Information Governance
Date:	18 December 2025

Appendix A: Police Force Parties

The Chief Officers of the Police Forces listed below are Parties to this DSA as represented by the NPCC.

Each Chief Officer is Controller under Data Protection Legislation for the processing of Personal Data by their organisation. Each Chief Officer is also a Party to the NPCC Collaboration Agreement.

Avon & Somerset Constabulary
Bedfordshire Police
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Derbyshire Constabulary
Devon & Cornwall Police
Dorset Police
Durham Constabulary
Dyfed-Powys Police
Essex Police
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
Humberside Police
Kent Police
Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Warwickshire Police
West Mercia Police
West Midlands Police
West Yorkshire Police
Wiltshire Police

Appendix B: Defined Terms Used in this DSA

Ad-Hoc Data Sharing – Sharing information not covered by a DSA on a one-off basis.

Controller/Data Subject/Criminal Offence Data/Personal Data/Special Category Personal Data – As defined in UK Data Protection Legislation

Data Protection Legislation – UK - All applicable Data Protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Information Commissioner or other relevant data protection supervisory body/regulator.

Non-UK - All applicable Data Protection and privacy legislation in force from time to time that applies to Controllers beyond the UK.

DSA – Data Sharing Agreement.

Data Sharing Lead – The point of contact in each Party for developing and maintaining the practical arrangements for data sharing under this DSA.

General Purposes – Any purpose other than a Law Enforcement Purpose.

General Processing – Processing (including sharing) of Personal Data for a General Purpose.

Law Enforcement Purposes – As defined by Section 31 Data Protection Act 2018 - the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Law Enforcement Processing – Processing (including sharing) of Personal Data for a Law Enforcement Purpose.

Lead Signatories – The Parties' strategic business leads who have confirmed the necessity of data sharing under this initiative.

NPCC – National Police Chiefs' Council as established under the NPCC Collaboration Agreement.

Parties – As set out on the Summary Page of this DSA.

Personal Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data which has been transmitted or stored or processed.

Personnel – Individuals undertaking data sharing activity for or on behalf of the parties, including: police officers, police staff, clergy, employees, contractors, and volunteers.

Providing Party – The Party who is the organisational source of Personal Data and shares it with one or more other Party. The Controller responsible for the initial collection of that data.

Sharing – Providing or disclosing data including Personal Data to another Party by any means and/or the receiving or collection of data including Personal Data from another Party by any means.

Subject Rights Application – The exercise by a Data Subject of their rights under the Data Protection Legislation

Appendix C: Illustrative Sharing Scenarios

This appendix is not used.

Appendix D: NPCC's Legal Basis for Sharing

Lawful Bases: NPCC

The NPCC's underlying power to share Personal Data is derived from (i) Common Law Policing Purposes which may be summarised as: protecting life and property, preserving order, preventing the commission of offences, and bringing offenders to justice and/or (ii) any duty or responsibility arising from statute or other rule of law including court order and royal prerogative.

In terms of UK Data Protection Legislation where the sharing is for one of the Law Enforcement Purposes the sharing falls under the scope of Part 3 of the Data Protection Act 2018 (DPA) with the NPCC acting as a competent authority.

Where the sharing is for purposes other than Law Enforcement Purposes (referred to as 'General Purposes') the sharing falls under the scope of the UK General Data Protection Regulation (UK GDPR).

Law Enforcement Purposes

Where the NPCC share or otherwise process Personal Data for one of the Law Enforcement Purposes:

The processing is necessary for the performance of a task carried out for a law enforcement purpose by the police acting as a competent authority (DPA Section 30).

Where sensitive processing is involved the processing is strictly necessary for a law enforcement purpose, an Appropriate Policy Document exists (DPA Section 42) and one the following DPA Schedule 8 conditions is met:

- the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest (DPA, Schedule 8(1))
- the processing is necessary to safeguard children and other individuals at risk. (DPA, Schedule 8(4))

General Purposes

Where the Police process Personal Data for General Purposes:

The sharing satisfies one of the following Processing Condition within UK GDPR Article 6(1):

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject.
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Where Special Category Data is shared, in addition to a UK GDPR Article 6(1) Processing Condition being met, one of the following UK GDPR Article 9(2) Special Processing Conditions apply:

- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- (g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Where Special Processing Condition (g) is chosen one or more of the following DPA Schedule 1 Part 2 substantial public interest conditions applies:

- (6) Statutory etc and government purposes – the sharing is necessary for a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.
- (7) Administration of justice – the sharing is necessary for the administration of justice.
- (10) Preventing or detecting unlawful acts – the sharing is necessary for the purposes of the prevention or detection of an unlawful act; must be carried out without the consent of the data subject so as not to prejudice those purposes; and is necessary for reasons of substantial public interest.
- (11) Protecting the public against dishonesty etc – the sharing is intended to protect members of the public against either dishonesty, malpractice or other seriously improper conduct, or unfitness or incompetence, or mismanagement in the administration of a body or association, or failures in services provided by a body or association; and must be carried out without the consent of the data subject so as not to prejudice those purposes; and is necessary for reasons of substantial public interest.
- (18) Safeguarding of children and of individuals at risk – the sharing is necessary for the purposes of protecting an individual aged under 18 or 18 or over at risk from neglect or physical, mental or emotional harm, or protecting their physical, mental or emotional well-being; must be carried out without the consent of the data subject; and is necessary for reasons of substantial public interest.

Where a condition in DPA Schedule 1 Part 1 or 2 is used an Appropriate Policy Document has been created and maintained by the NPCC in accordance with DPA Schedule 1 Part 4.

Where Criminal Offence Data is processed a compliance with UK GDPR Article 10 is also achieved, an Appropriate Policy Document has been created and maintained by the NPCC in accordance with DPA Schedule 1 Part 4, the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance, and one of the above DPA Schedule 1 Part 1, 2 or 3, conditions is met:

The Substantial Public Interest conditions required by the UK GDPR and Data Protection Act 2018 are met by the aims and objectives listed in Section 2 of this DSA.

Appendix E: SRA's Legal Basis for Sharing

The SRA is a company (Solicitors Regulation Authority Limited) registered in England and Wales (company registration number 12608059) whose registered office is at the Cube, 199 Wharfside Street, Birmingham B1 1RN.

It is the independent regulatory body responsible for the regulation of legal services by law firms and solicitors in England & Wales.

The SRA was formed in January 2007 by the Legal Services Act. The SRA's legal powers arise from various statutes and regulations including the Legal Services Act 2007, the Solicitors Act 1974, the Administration of Justice Act 1985, the Courts and Legal Services Act 1990 and the SRA's Standards and Regulations

The SRA investigates allegations of breaches of its requirements and where appropriate makes findings and imposes disciplinary sanctions. In more serious cases the SRA prosecutes allegations before the Solicitors Disciplinary Tribunal. The SRA also has the power to issue different types of criminal proceedings under the legislation dealing with the regulation of legal services.

The SRA has statutory and rule-based powers to require the production of documents or information, such as section 44B of the Solicitors Act 1974 and section 93 of the Legal Services Act 2007.

The SRA has a statutory power to share information with law enforcement under section 32(4) of the Solicitors Act 1974. The SRA cannot share information which is subject to legal professional privilege.

The SRA collect, use and share data primarily in the exercise of our regulatory functions. The lawful basis for processing this information is under UK GDPR as it is necessary for the exercise of official authority in the public interest.

The lawful basis for processing personal data under Article 6 Section 1(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The lawful basis for processing special categories of personal data under Article 9 Section 2(g) - processing is necessary for reasons of substantial public interest. The requirements of Section 10(3) of the Data Protection Act ('DPA') 2018, are met by para 11 of Part 2 of Schedule 1 of the DPA 2018 – 'protecting the public against dishonesty'.

Processing of personal data relating to criminal convictions is subject to Article 10 UK GDPR and Section 10(5) of the DPA. Article 10 requires that such processing (which is based on Article 6 (1) of the UK GDPR) is to be carried out "only under the control of the official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects."

Section 10 (5) of the DPA goes on to explain that "the processing meets the requirement in Article 10 (1) of the GDPR for authorisation by the law of the UK only if it meets a condition in Part 1, 2 or 3 of Schedule 1".

The most relevant such condition for the SRA, when processing details of convictions for internal regulatory processes, is the condition in paragraph 11 of schedule 1. This condition (Protecting the public against dishonesty etc.) provides for the retention and use of information relating to criminal convictions where it is "necessary" for the "exercise of a protective function……for reasons of a "substantial public interest……intended to protect members of the public against (a) dishonesty, malpractice or other seriously improper conduct (b) unfitness or incompetence.

There is therefore a clear legal basis under data protection legislation for us to request, retain and use information concerning (spent) criminal convictions and offences in order for us to exercise our regulatory powers in the public interest.