MEMORANDUM OF UNDERSTANDING (MoU)

For Public Sector Data Sharing within the UK

BETWEEN

THE HOME OFFICE

AND

Solicitors Regulation Authority (SRA)

In respect of: The exchange of information between the Professional Enabler Disruptions Team (PED) and the Solicitors Regulation Authority (SRA), where there are concerns regarding activity undertaken by solicitors or unregulated legal advisers.

Table of Contents

GLOSSARY

Definition	Interpretation
Controller	A person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures.: This covers a wide range of information about offenders or suspected offenders in the context of: • criminal activity; • allegations; • investigations; and • proceedings.
Data	Personal data, special category data and/or criminal offence/criminal conviction data as defined by the UK Data Protection Legislation and non-personal data.
Data Subject	The identified or identifiable living individual to whom personal data relates
European Convention on Human Rights (ECHR)	The European Convention on Human Rights (ECHR; formally the Convention for the Protection of Human Rights and Fundamental Freedoms) is an **international convention to protect human rights and political freedoms in Europe**
Data Protection Impact Assessment (DPIA)	A DPIA helps you to identify and minimise the data protection risks of a project or plan. It helps everyone involved in designing projects to think about privacy at the early stages
Freedom of Information Act	The Freedom of Information Act 2000 provides public access to information held by public authorities. The Act covers any recorded information that is held by a public authority in England, Wales, and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.
Human Rights Act 1998 (HRA)	The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. The Human Rights Act came into force in the UK in October 2000.
Information Commissioners Office (ICO)	The ICO is the UK's independent body that has been set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Memorandum of Understanding	MoU
Non-Personal Data	Non-personal data is any set of data which does not contain personally identifiable information. This in

	essence means that no individual living person can be identified directly or indirectly by looking at such data.
Personal Data	Means (as defined in the UK Data Protection Legislation) any data relating to an identified or identifiable living person ('data subject'). An identifiable person means a living individual who can be identified, directly or indirectly, in particular by reference to: a) an identifier such as a name, an identification number, location data, an online identifier or b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Privacy Information Notice (PIN)	Under data protection legislation the controller of personal data is required to provide data subjects with information about how the department processes or proposes to process their personal data. This is part of the fairness and transparency principle that underpins the UK GDPR. This information must be set out in a PIN issued under Article 13 or 14 of the GDPR.
Processor	Means a person, public authority, agency, or other body which processes personal data on behalf of the controller and is legally separate to the controller (i.e., not an employee or similar).
Processing	In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction).
Special Category Data	Special category data is data which the UK GDPR says is more sensitive, and so needs more protection. The UK GDPR defines special category data as: • data revealing racial or ethnic origin; • data revealing political opinions; • data revealing religious or philosophical beliefs; • data revealing trade union membership; • genetic data; • biometric data (where used for identification purposes); • data concerning health; • data concerning a person's sex life; and • data concerning a person's sexual orientation
UK General Data Protection Regulation (UK GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland, and Northern Ireland by

	virtue of section 3 of the European Union (Withdrawal) Act 2018
UK Data Protection Legislation	The "UK Data Protection Legislation" means: (a) the UK GDPR (b) the Data Protection Act 2018 (c) regulation made under the DPA 2018 (d) regulation made under section 2(2) of the European Communities Act 1972 which relate to the EU GDPR or the Law Enforcement Directive.

1. INTRODUCTION AND PARTICIPANTS TO THE MOU

1.1 THE SECRETARY OF STATE FOR THE HOME DEPARTMENT of 2 Marsham Street, London, SW1P 4DF hereafter referred to as the "**Home Office**" throughout this document.

1.2 Solicitors Regulation Authority, The Cube, 199 Wharfside Street, Birmingham, B1 1RN hereafter referred to as **"SRA"** throughout this document.

1.3 Collectively the Home Office and SRA are referred to as "Participants" and individually are referred to as a "Participant".

2. FORMALITIES

2.1 This MoU will come into effect on 09 June 2025

2.2 The date of the review of this MoU is 09 June 2026.

3. ROLE OF PARTICIPANTS

Role of Home Office

3.1 This is a link to the Home Office website, which provides information on the role of the Home Office.

Role of SRA

3.2 This is a link to the SRA website, which provides information on the role of the SRA. SRA | Who we are and what we do | Solicitors Regulation Authority

4. CONTROLLER STATUS OF HO AND SRA UNDER THE UK GDPR IN RESPECT OF PERSONAL DATA BEING SHARED UNDER THIS MOU

4.1 The Home Office is controller and primary owner of the Home Office data transferred to SRA under this MoU. Once the SRA has received and reviewed the data they will, when appropriate use it to support their investigations. At this time, they will become the controller of the data.

4.2 The SRA is Controller and primary owner of the SRA data transferred to the Home Office under this MoU. Upon receiving this data, the Home Office will use this data to support their investigations. At this time, they will become the controller of the data.

5.TYPE OF DATA SHARING ACTIVITY

5.1 The Home Office and the SRA will share data as and when required, expected to be on a regular basis. This will involve reciprocal exchange of data between both.

6. PURPOSE AND INTENDED BENEFITS OF DATA SHARING

Purpose

6.1 To allow the Home Office to share data with the Solicitors Regulation Authority (SRA) where there are concerns regarding activity undertaken by solicitors.

There will be two types of information exchanges between the Home Office and the SRA, where:

- Home Office intelligence receive referrals made by caseworkers and members of the public; the referrals will be developed before being disseminated to the SRA.
- the SRA request Home Office intelligence to provide them with evidence they hold in relation to individuals or law firms subject to regulatory investigation.

This processing will:

- enable the Home Office and the Solicitors Regulation Authority (SRA) to carry out their stated functions.
- prevent and/or detect fraud or other criminal activity against the Home Office and the Solicitors Regulation Authority
- ensure that individuals and firms regulated by the Solicitors Regulation Authority operate independently and with integrity in the interests of their clients and in the wider public interest.
- be necessary and for a legitimate purpose in accordance with purpose limitation data protection principle of the UK GDPR Article 5 1(b) Personal data shall be*:" collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');"*

Intended Benefits

6.2 The Home Office and the SRA will benefit from this data exchange as it will help support the prevention and detection of fraud and other criminal activity against the Home Office and the Solicitors Regulation Authority. Sharing this data with the SRA ensures that individuals and firms regulated by them operate independently and with integrity in the interests of their clients and in the wider public interest.

7. LEGAL CONSIDERATIONS- LEGAL POWERS

Home Office

7.1 As a Crown Department, the Home Office will also rely on Common Law powers to share the personal information with SRA to combat illegal migration abuse and safeguard applicants.

SRA

7.2 The SRA is the independent regulatory body responsible for the regulation of legal services by law firms and solicitors in England and Wales. As the regulatory body for solicitors in England and Wales, the SRA is required to exercise its statutory and regulatory functions in order to protect the public from misconduct, unfitness to practice or incompetence by solicitors.

7.3 The SRA's powers arise from various statutes and regulations including the Solicitors Act 1974, the Administration of Justice Act 1985, the Courts and Legal Services Act 2007 and the SRA's Standards and Regulations. The SRA collects, uses and shares data primary in the exercise of its regulatory functions.

8. LEGAL CONSIDERATIONS- LAWFUL BASES

Home Office

8.1 The Home Office's lawful basis for the transfer of personal data to SRA is **UK GDPR Article 6 (1)(e) (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".*** Article 6(1) (e) basis includes processing of personal data that is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department. The Home Office believes that it is in the public interest to investigate claims of representative abuse in order to protect against threats to public security and safety.

8.2 The Home Office's Legal basis for the transfer of special category data with the SRA is **UK GDPR Article 9,** substantial Public Interest.

SRA

8.3 The SRA's lawful basis for processing this information is under UK GDPR Article 6 Section 1(e) as it is necessary for the exercise of its official authority in the public interest.

8.4 The SRA's lawful basis for processing special category data is under UK GDPR Article 9 Section 2(g) as it is necessary for the reasons of substantial public interest.

8.5 As the regulatory body for solicitors in England and Wales, the SRA is required to exercise its statutory and regulatory functions in order to protect the public from misconduct, unfitness to practice or incompetence by solicitors.

9. FAIRNESS/TRANSPARENCY

Home Office

9.1 The data on Home Office applicants is collected in line with the Borders Immigration and Citizenship System (BICS) Privacy Information Notice (PIN). The PIN sets out that data may be shared by the Home "to assist other organisations to deliver their statutory functions". It also states that personal information will be processed in order to detect and prevent detect and investigate crime. The BIC PIN can be accessed here: borders-immigration-and-citizenship-privacy-information-notice

SRA

9.2 The SRA sets out how and why data is collected, processed, shared and the rights of data subjects in its privacy notice. The privacy notice can be accessed here: SRA | Privacy notice | Solicitors Regulation Authority

10.THIRD PARTY PROCESSING

10.1 N/A

11. DATA PROTECTION IMPACT ASSESSMENTS

11.1 A Data Protection Impact Assessment has been completed.

11.2 Date DPIA completed 25 October 2023.

12. DATA/ INFORMATION TO BE SHARED

12.1 Home Office

List of Data Items/fields	Category of Personal data	Cohorts
• Names of solicitor's firm.	Non personal data.	SRA regulated solicitors' firms. Unregulated organisations.

• Names of Individual solicitors.	Personal data.	SRA regulated solicitors. Unregulated legal advisers.
• First name/ Surname.	Personal data.	All migrants that have submitted asylum and/ or immigration applications.
• DOB	Personal data.	All migrants that have submitted asylum and/ or immigration applications.
• Address	Personal data.	All migrants that have submitted asylum and/ or immigration applications.
• Gender	Personal data.	All migrants that have submitted asylum and/ or immigration applications.
• Nationality	Personal data.	All migrants that have submitted asylum and/ or immigration applications.
• Documents detailing asylum and/ or immigration matters.	Sensitive data.	All migrants that have submitted asylum and/ or immigration applications.
• Race or ethnic origin (including nationality)	Personal Data	All migrants that have submitted asylum and/ or immigration applications.
• Health	Sensitive Data Special category	All migrants that have submitted asylum and/ or immigration applications.
• Sexual orientation	Sensitive Data	All migrants that have submitted asylum and/ or immigration applications.
• Religious or philosophical beliefs	Sensitive Data	All migrants that have submitted asylum and/ or immigration applications.

12.2 SRA

List of Data Items/fields	**Category of Personal data**	**Cohorts**
• Names of solicitor's firm.	Non personal data.	SRA regulated solicitors' firms. SRA register/CRM. Unregulated organisation.

• Names of Individual solicitors.	Personal data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• First name/ Surname.	Personal data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• DOB	Personal data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Address	Personal data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Gender	Personal/Sensitive data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Nationality	Personal/Sensitive data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Documents relating to investigation.	Personal/Sensitive data.	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Race or ethnic origin	Personal/Sensitive Data	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Health	Personal/Sensitive Data	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Sexual orientation	Personal/Sensitive	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.
• Religious or philosophical beliefs	Personal/Sensitive Data	SRA regulated solicitors. SRA register/CRM. Unregulated legal advisers.

13. PROCESS FOR DATA SHARING

Volume
13.1 The volume of personal data being shared with the SRA is expected to exceed 1000 pieces of personal data over a 12-month period**.**
Duration
13.2 Data will be shared between the Home Office and SRA from 8th January 2024 for up to five years
Source(s) of the data

13.3 The data shared will be sourced from Home Office immigration systems including ATLAS, HOPS, CRS, SMS, Entity, CID.
Frequency
13.4 Data will be supplied to the SRA if and when it is requested or required.
Format
13.5 The data will be formatted as PDFs, Word documents JPEGs, or in some instances an Excel worksheet.
Means of transfer of the data
13.6 Home Office Data will be stored in the PED SharePoint; access is restricted to members of the team. Data will primarily be transferred to the SRA via a government approved email address. SRA have provided a CJSM email address, confirmed to be a secure email address by the Home Office Cyber Security team. In instances where the information provided to the SRA by the Home Office exceeds the size limit allowed by the CJSM email address then this can be uploaded to a secure Teams channel. Access to the specific channel is controlled and only limited numbers of SRA staff approved by PED have the ability to access it Home Office Cyber Security have confirmed that permitting authorised members of the SRA access to the secure Teams channel is allowed for the purpose of viewing the relevant information. **13.7 SRA** Requests for further information from the SRA will be sent via a government approved email address to an inbox restricted to authorised PED team members. When sending data from the SRA to the PED, data will either be transferred by hard copy or by Mimecast large fileshare or via CJSM (secure email).
Government Security Classification
13.8 Government security classification will be OFFICIAL SENSITIVE for all data.

14. ACCURACY

Quality and Accuracy

14.1 The accuracy of the data being shared is dependent on the inputs from the legal representatives and the applicant, we are sharing this information as we

suspect it's not accurate. Prior to transferring to the SRA the data's accuracy will be evaluated through quality control checks. This will be actioned by a Higher Executive Officer in PED, to ensure the data is not only delivered in the correct format but also meets the criteria of adequacy, relevance to the request and is limited has been limited to what is necessary.

Notification of errors in the data/information shared.

14.2 Checks will be carried out prior to the data being transferred however where errors are identified after transfer, the disclosing participant will notify the receiving participant of any errors within 5 working days of discovery to the designated point of contact for this data sharing activity detailed in Annex A.

Rectification

14.3 If inaccurate data is transferred to the SRA, we will ask for this data to be destroyed by the SRA and confirm with Home Office point of contact when this had been actioned.

15. DATA SECURITY

Security Standards

15.1 Participants must ensure effective measures are in place to protect personal data in their care and manage potential or actual incidents of loss of the personal data. Such measures will include, but are not limited to:

- Participants will take steps to ensure that all staff are adequately trained and are aware of their responsibilities under the Data Protection Legislation and this MoU.
- Access to personal data received by Participants pursuant to this MoU must be restricted to personnel on a legitimate need-to-know basis, and with security clearance at the appropriate level.
- Participants will comply with the Government Security Classifications Policy (GSCP) where applicable.

Home Office

15.2 Once data has been collated by caseworkers it will be saved to the PED SharePoint, when appropriate the data will then be transferred to the SRA's secure email inbox or made available to them via the secure Teams channel. Home Office Cyber Security have been consulted and confirmed that the CJSM email address immigration.intel@solicitorsra.cjsm.net supplied by the SRA permits the sending of Official Sensitive emails from government approved systems such as a Home Office email address.

15.3 Data stored in the Professional Enabler Disruptions SharePoint is only accessible to authorised members of the team. All staff involved in this data sharing

activity will possess SC security clearance. Once the data is prepared to be shared with SRA it will be sent via PEDRegulatorReferrals@homeoffice.gov.uk

15.4 Requests for information sent by the SRA will be received into a secured government email inbox PEDRegulatorReferrals@homeoffice.gov.uk Only members of the PED team will have access to this inbox and will possess SC security clearance.

SRA

15.5 The SRA's Intelligence Unit will be the sole point of contact for sharing information between the PED and the SRA. Information will be transmitted via the email addresses detailed above.

15.6 The SRA's Intelligence Unit stores data within SRA systems in a restricted access part of those systems. Only members of the SRA Intelligence Unit have access to this information. All Unit members possess SC security clearance.

15.7 Once the data has been collated, the SRA Intelligence Unit may share relevant data with other staff within the SRA for the purposes of initiating or assisting in SRA investigations. Any data shared will be subject to specific handling restrictions as to its use.

16. FACILITATING THE EXERCISE OF THE RIGHTS OF DATA SUBJECTS

16.1 In the event a data subject right request relating to the Personal Data shared under this MoU is received by either Participant; they will individually consult with each other on the proposed response and respond to the request in accordance with the UK Data Protection Legislation, and in accordance with their respective organisation's internal procedures for responding to data subject right requests.

16.2 Where a request is received to rectify, erase, or restrict any Personal Data shared under this MoU; the receiving Participant will communicate any rectification or erasure of Personal Data or restriction of processing carried out in accordance the UK Data Protection Legislation to the other Participant, where it is possible and proportionate to do so.

16.3 The contact for responding to Data Subject Right requests for the Home Office is provided at **Annex A**.

16.4 The contact for responding to Data Subject Right requests for SRA is provided at **Annex A.**

17. FREEDOM OF INFORMATION REQUESTS

17.1 Home Office and SRA shall assist and co-operate with each other to enable each department to comply with their information disclosure obligations. In the event

of one Participant receiving a FoI request that involves disclosing information that has been provided by the other Participant, the Participant in question will notify the other to allow it the opportunity to make representations on the potential impact of disclosure and will issue a formal response following its internal procedures for responding to FoI requests within the statutory timescales.

17.2 The SRA is not subject to the provisions of the FoI but as a transparent regulator the SRA applies their own Transparency Code in the similar way as the FoI.

17.3 The contact for responding to FoI requests for the Home Office is provided at **Annex A.**

17.4 The contact for responding to FoI requests for SRA is provided at **Annex A.**

18. DATA RETENTION / DELETION PROCESS

Home Office

18.1 Data received from SRA will be stored in a secure SharePoint file, access will be restricted to staff within Professional Enabler Disruptions Team. Home Office will hold data received from the SRA as per Home Office's document retention policy for the function and legal activity for which the data was shared (i.e., for as long as is required for completion of the data sharing). Once this date has passed, any SRA information will be destroyed securely in accordance with Home Office destruction policies and in accordance with HMG Security Policy Framework. HO will verify to SRA that this has been completed.

SRA

18.2 SRA will only keep personal data as long as necessary to ensure it can fulfil their regulatory role in the public interest in line with their retention policy. Once this date has passed, any data will be destroyed securely in accordance with SRA internal destruction policies, and the UK Data Protection Legislation. SRA will verify to Home Office that this has been completed.

18.3 Guidance stipulating data retention periods for the SRA can be found here: SRA | Record retention schedules | Solicitors Regulation Authority

19. ONWARD DISCLOURES TO THIRD PARTIES

Home Office

19.1 N/A

SRA

19.2 the SRA will ensure that any onward disclosures are lawful and only relevant data is shared that is necessary for the purpose of the sharing.

20. COMPLAINT HANDLING

Complaints

20.1 The Participants will work together regarding the response to any complaint received related to the data sharing activity set out in this MoU.

Disputes Resolution

20.2 If either Participant has any issues, concerns, or complaints about this MoU it will notify the other and they will, acting in good faith, seek to resolve the issue by negotiations between themselves.

20.3 Contact details for day-to-day operational queries or issues/disputes relating to the data sharing activity set out in this MoU should be directed to the designated contacts provided in **Annex A** for each Participant.

21. MONITORING AND REVIEWING ARRANGEMENTS

21.1 This MoU must be reviewed on an annual basis unless a significant change on the side of either participant is identified.

21.2 Reviews outside of the proposed review period can be called by representatives of either Participant.

21.3 The MoU review process will focus on:

- whether the MoU is still necessary and fit for purpose,
- whether the existing data sharing arrangements should be extended or amended,
- whether the lawful bases relied upon by the Participants for sharing the data remain valid, including whether any legislation has been amended or enacted that would impact on any purpose-specific information sharing activities. If a Participant's lawful basis for information sharing has changed, the data sharing MoU will need to be amended to reflect this.

21.4 In the event of a personal data breach or other breach of the terms of this MoU any of the Participants, this MoU must be reviewed immediately by the Participants and termination of the data sharing arrangement considered.

21.5 A record of all reviews will be created and retained by each Participant (see Annex B).

22. COSTS

22.1 N/A

23. TERMINATION

23.1 This MoU may be terminated by giving 3 months' notice by either Participant.

23.2 The Participants to this MoU reserve the right to terminate this MoU with three months' notice in the following circumstances:

- by reason of cost, resources, or other factors beyond the control of the Home Office or the SRA.
- if any material change occurs which, in the opinion of the Home Office and the SRA following negotiation significantly impairs the value of the data sharing arrangement in meeting their respective objectives.

23.3 The Participants to this MoU reserve the right to terminate or suspend this MoU immediately without notice in the following circumstances:

- in the event of a serious breach of the terms of this MoU,
- inappropriate, unlawful or misuse of data shared under this MoU.

23.4. Where a decision is made to terminate the MoU due an incident as described in paragraph 22.3 above, the participant responsible for the incident must immediately return or delete any copies of data received under this MoU. Where data shared under this MoU is deleted, the participant responsible for the incident must provide evidence to the disclosing participant of deletion.

23.5 Contact details for notification and handling of such serious incidents are provided at **Annex A.**

24. DATA BREACHES / INFORMATION SECURITY BREACHES

Home Office

24.1 Personal Data / Security breaches, including misuse of Home Office information shared under this MoU must be reported to the contact provided at Annex A within 24 hours of becoming aware of the breach and no later than 72 hours.

Solicitors Regulation Authority

24.2 Personal Data/Security breaches, including misuse of SRA information shared under this MoU must be reported to the contact provided at Annex A below within 24 hours of becoming aware of the breach and no later than 72 hours.

25. SIGNATORIES

Signed on behalf of the Home Office:

25.1 I accept the terms of the Memorandum of Understanding on behalf of the Home Office.

Signature:	
Name:	
Position:	G6 Head of Operations PED
Date:	21 May 2025

Signed on behalf of the Solicitors Regulation Authority:

25.2 I accept the terms of the Memorandum of Understanding on behalf of the Solicitors Regulation Authority.

Signature:	
Name:	Andrew Turton
Position:	Director of Risk and Information Governance
Date:	09 June 2025

ANNEX A – Business Contacts

Business as Usual Contacts – Home Office

Contact (Name and Position)	Email	Responsibility
Head of operations PED Home Office	PEDRegulatorReferrals@homeoffice.gov.uk	Operational Queries/ Resolving Data Quality Issues/Disputes/ Resolution
Head of operations PED Home Office	PEDRegulatorReferrals@homeoffice.gov.uk	Review and amendments to MoU
Law enforcement Lead PED Home Office	PEDRegulatorReferrals@homeoffice.gov.uk	Personal data Breach/Security Breach
Law enforcement Lead PED Home Office	PEDRegulatorReferrals@homeoffice.gov.uk	Freedom of Information Act Requests
Law enforcement Lead PED Home Office	PEDRegulatorReferrals@homeoffice.gov.uk	Data Subject Right Requests

Business as Usual Contacts – Solicitors Regulation Authority

Contact (Name and Position)	Email	Responsibility
Christopher Hall Intelligence Manager	intel@sra.org.uk	Operational Queries/ Resolving Data Quality Issues/Disputes/ Resolution
Christopher Hall Intelligence Manager	intel@sra.org.uk	Review and amendments to MoU
Andrew Turton Data Protection Officer	srainformationcompliance@sra.org.uk	Personal data Breach/Security Breach

Andrew Turton Data Protection Officer	srainformationcompliance@sra.org.uk	Freedom of Information Act Requests
Andrew Turton Data Protection Officer	srainformationcompliance@sra.org.uk	Data Subject Right Requests

Annex B – Document Control

Document Control Personnel

Key Personnel	Name and Position	Organisation (Team)
Author	Law Enforcement Lead, PED.	Home Office

Version and review history

Version	Date	Summary of changes	Changes Marked
Draft 0.1	08/12/2023	Amended points following review.	
Draft 0.2	07/06/2024	Review and amendments made by SRA	
Draft 0.3	12/06/2024	Amendments made by Grade 7	
Draft 0.4	17/06/2024	Finalised copy to send for review	
Draft 0.5	28/06/2024	Review of draft	No
Draft 0.6	13/09/2024	SRA amendments to comments	No
Draft 0.7	28/03/2025	SRA amendments and sign off.	
Final v1.0	09/06/2025	Signed and in operation	