



Memorandum of Understanding (Process)
between
HMRC Customer Compliance Group –ISBC Agents & Technical
Compliance (A&TC)
HMRC Solicitor’s Office and Legal Services
and
Solicitors Regulation Authority
for
Public Interest Disclosures pursuant to the Commissioners’
General Instruction (Misconduct Disclosures for Legal
Professionals)

The process MoU register ID / reference is: [Click or tap here to enter text.](#)

Table of Contents

1. Participants to the MoU	3
2. Introduction.....	3
3. Purpose and benefits of the data sharing agreement.....	4
4. Type of data being shared under this agreement.....	5
5. Data Protection Impact Assessment (DPIA)	5
6. Relationships under UK GDPR in respect of any personal data being exchanged under this agreement .	6
7. Handling of Personal Data and Security	6
8. Duration, Frequency and Volume of the data sharing (To be completed by HMRC)	7
9. Legal considerations and basis to share data between the Participants	7
10. Lawful basis under UK GDPR to process personal data	9
11. Data to be shared and systems it will be derived from	9
12. How the data will be shared (to be completed by HMRC and where applicable OGD / PSB).....	9
13. Accuracy of the data being shared.....	10
14. Retention and Destruction of data.....	10
15. Onward disclosure to third parties.....	11
16. Role of each Participant to the MoU	11
17. Monitoring and Reviewing and arrangements.....	12
18. Assurance Arrangements	13
19. Security Breaches, Security Incidents or loss or unauthorised disclosure of data	13
20. Subject Access Requests	13
21. Freedom of Information Act (FOI) 2000	14
22. Issues, disputes, and resolution.....	14
23. Costs	14
24. Termination	14
25. Signatories	15
26. Appendices and Annexes	15

1. Participants to the MoU

HM Revenue & Customs are referred to as Participant 1 and Solicitors Regulation Authority are referred to as Participant 2. Collectively they are referred to as the "Participant(s)".

1.1 Participant 1 - HM Revenue & Customs		
His Majesty's Revenue & Customs, of 100 Parliament Street, London, SW1A 2BQ		
	Contact 1	Contact 2
HMRC Directorate	ISBC A&TC	ISBC A&TC
Name of business contact	Edwige Hill	Tommy Robinson
Role	ISBC A&TC Deputy Director	ISBC A&TC Assistant Director - Specialist
Email address	edwige.hill@hmrc.gov.uk	thomas.robinson@hmrc.gov.uk
Telephone Number	03000 520899	03000 581131

1.2 Participant 2 – Solicitors Regulation Authority		
Solicitors Regulation Authority, The Cube, 199 Wharfside Street, Birmingham, B1 1RN		
	Contact 1	Contact 2
Directorate	Risk and Information Governance	Intelligence
Name of business contact	Andrew Turton	Christopher Hall
Role	Director	Intelligence Manager
Email address	Andrew.Turton@sra.org.uk	Christopher.Hall@sra.org.uk
Telephone Number		

2. Introduction

2.1 This MoU sets out the information sharing arrangement between the aforementioned participants. For the purposes of this MoU, 'information' is defined as a collective set of Data and/or facts that when shared between the Participants through this MoU will support the participants in delivering the purpose of the data sharing activity described in section 3 below.

2.2 Information will only be exchanged between the participants where it is lawful to do so. The relevant legal authorities are detailed within this agreement. It should be noted that 'exchange' includes all transfers of information between the participants.

2.3 This MoU is not legally binding. This MoU should not be interpreted as removing, or reducing, any of the existing legal obligations or responsibilities of each participant, for example as controllers under the UK General Data Protection Regulations (UK GDPR). Nothing in this MOU shall, or is intended to:

- a) create any legal or procedural right or obligation which is enforceable by either participant against the other; or
- b) create any legal or procedural right or obligation which is enforceable by any third party against either of the participants or against any other third party or
- c) prevent either of the participants from complying with any law which applies to them; or
- d) fetter or restrict in any way whatsoever the exercise of any discretion which the law requires or allows the participants to exercise or
- e) create any legislative expectation on the part of any person that either of the participants to this MOU will do any act (either at all, or in any particular way, or at any particular time) or will refrain from doing any act.

Nonetheless the participants are genuinely committed to pursuing the aims and purposes of this MOU in good faith and intend to act in accordance with its terms on a voluntary basis.

2.4 A glossary of terms, definitions of abbreviations of this MoU are detailed in Annex A of this MoU.

3. Purpose and benefits of the data sharing agreement

3.1 Describe the purpose of the MoU and the participants' views of why it is necessary and proportionate.

HMRC and the SRA consider that the disclosure of information to each other pursuant to this MOU is necessary and proportionate because it will;

- assist both parties in their investigation or supervision work in the public interest so far as such assistance is lawful;
- provide a framework for the lawful disclosure of information between the two organisations and
- set out the legal framework under which both organisations may lawfully disclose information to each other.

3.2 What are the specific aims of the data sharing agreement?

See above.

3.3 How will the data being shared help achieve those aims?

Where it is lawful and in the public interest to do so, the participants agree to disclose the necessary and relevant information to each other. This will:

- a). enable the assessment of risk to the public such as to:
 - i. minimise the risk of financial default.

- ii. protect vulnerable clients or beneficiaries.
- iii. minimise the risk of fraud or other criminality; and
- iv. identify the risk of financial failure.

b). enable alleged criminality, misconduct, breaches of the SRA principles, or other failures to be properly investigated and decided upon.

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

d). assist with regulatory, disciplinary, or other legal proceedings, whether held in public or not.

provided that the recipient is reasonably considered able to take regulatory or other proper action upon the information.

The minimum amounts of data should be shared between the two organisations and should only be escalated to allow both organisations to complete their statutory roles.

3.4 Describe the benefits that the Participants hope to bring to individuals or society or the wider impact e.g. reduction in fraud and debt, supports UK economy, benefits HMRC customers etc

The benefits that the participants hope to achieve include:

- The raising of standards across the wider tax agent profession by addressing misconduct within the legal profession in compliance with the SRA's regulatory objectives, therefore promoting compliance, protecting customers and assisting with closing the tax gap.
- The establishment of equivalent measures within HMRC in respect of how misconduct in the legal and accountancy professions is addressed.
- The promotion of good stakeholder relationships between HMRC and the SRA ensuring that prompt and effective action can be taken to identify, investigate and address serious and significant misconduct.
- The establishment of clear mechanisms which enable HMRC legal professionals to comply with regulatory obligations to report any facts or matters capable of amounting to a serious breach of regulatory arrangements whilst ensuring that confidentiality and information disclosure obligations are respected. This will avoid any potential conflict between legal and professional obligations.

4. Type of data being shared under this agreement

4.1 Does this MoU agreement involve the exchange of Personal Data?

Yes (Go to section 5)

No (Select 'N/A – No Personal data' for Sections 5 to 7 and go to Section 8)

5. Data Protection Impact Assessment (DPIA)

N/A - No Personal Data

5.1 HMRC - Have you completed a Data Protection Impact Assessment (DPIA)?

Yes <input checked="" type="checkbox"/>	DPIA Reference Number:	12760
	Date DPIA was registered:	23/07/2024
	Date DPIA was last reviewed:	23/07/2024
No <input type="checkbox"/>	<i>Please ensure a DPIA is completed before you exchange any personal data. You will not be authorised to transfer data until one has been completed.</i>	

5.2 SRA - Have you completed a Data Protection Impact Assessment (DPIA)?		
Yes <input type="checkbox"/>	DPIA Reference Number:	Click to insert reference here
	Date DPIA was registered:	Click or tap to enter a date.
	Date DPIA was last reviewed:	Click or tap to enter a date.
No <input checked="" type="checkbox"/>	<i>The processing is not considered high risk and a DPIA is not required. Disclosures will be dealt with on a case by case basis and any risks can be considered at that stage.</i>	

6. Relationships under UK GDPR in respect of any personal data being exchanged under this agreement N/A – No Personal Data

6.1 Status of HMRC under UK GDPR
<p>HMRC will be disclosing and receiving personal data under this agreement.</p> <p>Where personal data is being disclosed under this agreement, HMRC's status will be a controller because HMRC separately determines the purpose and means of the processing of the personal data.</p>

6.2 Status of SRA under UK GDPR
<p>SRA will be disclosing and receiving personal data under this agreement.</p> <p>Where personal data is being received under this agreement, SRA status will be a controller because they separately determine the purpose and means of the processing of the personal data after transfer.</p>

7. Handling of Personal Data and Security N/A – No Personal Data

7.1 Where participants bear the responsibility of a Data Controller (see Section 6.1 and 6.2), they must ensure that any personal data received pursuant to this MoU is handled and processed in accordance with data protection legislation and appropriate security standards

7.2 Additionally as part of the Government, HM Revenue & Customs must process personal data in compliance with the mandatory requirements set out in HM Government [Security Policy Framework](#) guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying Information assets. The SRA agrees must process data in line with DPA 2018.

7.3 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:

- personal data should not be transferred or stored on any type of removable media unless absolutely necessary, and if so, it must be encrypted, and password protected to an agreed standard
- participants will take steps to ensure that all staff involved in the data sharing activities are adequately trained and are aware of their responsibilities under the DPA, UK GDPR 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 and
- HM Revenue and Customs will comply with the [Government Security Classifications Policy \(GSCP\)](#), and the SRA with DPA 2018.

8. Duration, Frequency and Volume of the data sharing (To be completed by HMRC)

Date MoU comes into effect:	01/08/2024
Date by which MoU needs to be formally reviewed:	31/07/2025
Date MoU will cease to be valid:	31/07/2027
Frequency & Volume of data being shared:	As necessary and appropriate for the professional regulator to carry out their investigation.

9. Legal considerations and basis to share data between the participants

9.1 HMRC has specific legislation within the [Commissioners for Revenue and Customs Act \(2005\)](#) which covers the confidentiality of information held by the department, when it is lawful to disclose that information and legal sanctions for wrongful disclosure. For HMRC, disclosure of information is precluded except in certain limited circumstances (broadly, for the purposes of its functions, where there is a legislative gateway or with customer consent). Unlawful disclosure relating to an identifiable person constitutes a criminal offence. The criminal sanction for unlawful disclosure is detailed at section 19 of the Commissioners for Revenue and Customs Act 2005.

9.2 Data can only be shared where there is a legal basis for the exchange and for the purposes described in this MoU as specified at Section 10 below. No data should be exchanged without a legal basis and all exchanges must comply with our legal obligations under UK GDPR, the Data Protection Act 2018 and Human Rights Act (HRA) 1998.

9.3 Enter relevant legal basis / bases for HMRC to disclose data

Section 18 of the Commissioners for Revenue and Customs Act (CRCA) sets out the specific circumstances in which HMRC may disclose information. These are:

- where HMRC has a statutory legal gateway permitting the disclosure of information to a third party;
- for the purposes of HMRC's functions;
- where the person or organisation that the information relates to has given their consent¹;
- where disclosure is for the purposes of civil proceedings or criminal investigation or proceedings;
- where disclosure is made in pursuance of a court order binding on the Crown;
- where disclosure is to a body with the statutory power in CRCA to inspect HMRC; or
- where disclosure is made in specific circumstances that are defined as being in the 'public interest' as set out in CRCA.

Section 20(1)(a) of CRCA 2005 allows for disclosure in the public interest as mentioned in section 18(2)(b) of CRCA 2005 if the disclosure is made on the instructions of the Commissioners (general or specific). A General Instruction setting out the process to permit misconduct disclosures about legal professionals was approved by the Commissioners on 21 October 2021.

Section 20(3) of CRCA 2005 applies to a disclosure if:

- it is made to a body which has responsibility for the regulation of a profession
- it related to misconduct on the part of a member of the profession and
- the misconduct relates to a function of the Revenue and Customs. CRCA.

Any disclosure of information by HMRC under s.20(3) CRCA 2005 to the SRA must conform to the relevant general instruction published by the Commissioners.

Information disclosed to the SRA by virtue of s.20(3) CRCA 2005 must not be further disclosed without first obtaining the consent of the Commissioners.

HMRC can also disclose information to the SRA if a High Court order is obtained to enforce an order made under section 44B Solicitors Act 1974 or an order made pursuant to S44BB, related or analogous legislation. Court orders are an exception to HMRC's duty of confidentiality under section 18(2)(e) CRCA 2005.

9.4 Relevant legal basis / bases for the SRA to disclose data

The SRA is the independent regulatory body responsible for the regulation of legal services by law firms and solicitors in England and 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 collects, uses and shares/discloses data primarily in the exercise of its regulatory functions. Its lawful basis for processing this information is under UK GDPR is Article 6 Section 1(e) as it is necessary for the exercise of its official authority in the public interest.

10. Lawful basis under UK GDPR to process personal data N/A – No Personal Data

10.1 Personal data can only be processed (transferred, disclosed) where there is a valid lawful basis/bases as set out in Article 6 of UK GDPR – see [ICO Guidance](#)

10.2 Enter relevant lawful basis for HMRC to process (share) personal data

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

10.3 If applicable - Enter relevant lawful basis for the SRA to process (share) personal data

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

11. Data to be shared and systems it will be derived from

11.1 Describe the types of data / data fields being shared and their source systems

Where misconduct has been identified by HMRC, information and evidence will be extracted from relevant internal systems of HMRC and will form part of a report to be sent to the SRA which will be subject to the internal processes detailed in Annex E. Disclosure of the material will ultimately be authorised by a SOLS Director and a Deputy Director from the Tax Administration Directorate on consideration of the specific circumstances.

11.2 What is the Government Security Classification for the data being shared?

Official Sensitive

11.3 Is there any special category data, sensitive data or criminal offence data being shared?

Yes

No

Certain types of misconduct could potentially constitute an allegation of a criminal offence. No special category data will be disclosed unless it is necessary for the SRA to fulfil their functions with respect to the alleged misconduct.

12. How the data will be shared (to be completed by HMRC and where applicable OGD / PSB)

12.1 Describe the method by which data will be transferred under this agreement

When sending data from HMRC to the SRA, data will either be transferred by hard copy or by SDES (Secure Data Exchange Service).

SDES is HMRC's preferred secure method of transferring data and allows users to request, move, and manage their data with a personalised dashboard while also providing a history of users' data movements in one place.

When data is transferred by hard copy it will be sent via 'Tracked' post with a signature required upon delivery.

When sending data from the SRA to HMRC, data will either be transferred by hard copy or by Mimecast large fileshare or via CJSJ (secure email). Removable media will only be used where absolutely necessary and provided that it is encrypted to an agreed standard.

When data is transferred by hard copy it will be sent via 'Tracked' post with a signature required upon delivery.

12.2 Will direct (or browser) access to HMRC systems be granted?

Yes

No

13. Accuracy of the data being shared

13.1 Before sharing data both Participants must take all reasonable steps to ensure that the data being shared is both accurate and up to date.

13.2 The exporting department will ensure that data integrity meets their own department's standards, unless more rigorous or higher standards are set out and agreed at the requirements stage.

13.3 Participants will notify each other of any inaccuracies of the data as they are identified.

14. Retention and Destruction of data

14.1 State how long the data will be retained for by each Participant and what their arrangements are for secure storage, and disposal / destruction of data.

Information held by HMRC will be retained in accordance with existing retention policies, typically for 6 years from date of last use for HMRC and 7 years from the date of case closure for the SRA. If the information becomes part of the SRA investigation records, we will then retain in line with the published SRA retention policy.

14.2 State what access controls each Participant will have in place to ensure access to the data will only be provided to authorised personnel with the appropriate security clearance.

The SRA's Intelligence Department is the point of contact for sharing information with HMRC and the team will only share the necessary information within the SRA when there is a genuine business need

15. Onward disclosure to third parties

15.1 The SRA agrees to seek permission from HM Revenue & Customs before any onward disclosure of information to a third party and will only disclose any information if permission is granted.

15.2 Where permission for onward disclosure is granted by HMRC, describe how the onward transfer of information from the SRA to the third party will be handled (if allowed) under the legal basis

Save for a disclosure made for purposes required by law, the SRA will not disclose information to any outside organisation without the prior approval of HMRC.

Where a disclosure is made which is required by law, the SRA will inform HMRC of that disclosure.

HMRC will not disclose information supplied by the SRA to any outside organisation unless permitted or required by law and will not make any such disclosure without prior approval by the SRA.

16. Role of each Participant to the MoU

16.1 Role of HMRC

- Identify the appropriate data required from HM Revenue & Customs IT systems / records
- Provide the data to Participant 2 in a **report** transferred by **SDES**, or in hard copy where absolutely necessary, from and to agreed contact points
- Only allow access to that data by the team requiring it
- Ensure that staff handle this data in line with the approved secure transfer method agreed by both departments and within HM Revenue & Customs data security instructions
- Only store the data for as long as there is a business need to do so
- Move, process and destroy data securely i.e. in line with the principles set out in HM Government [Security Policy Framework](#), issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information.
- Comply with the requirements in the [Security Policy Framework](#), and in particular prepare for and respond to Security Incidents and to report any data losses, wrongful disclosures or breaches of security relating to information.
- The disclosing party also agrees to notify the recipient of:
 - any restrictions on the use to which the information can be put, and
 - any restrictions which apply to the onward disclosure of the information, and

in the absence of such notification, the receiving party may assume that there are no such restrictions (in addition to any restrictions that apply as a matter of law).

16.2 Role of the SRA

- Identify the appropriate data required from HM Revenue & Customs.
- Only use the information for purposes that are in accordance with the legal basis under which it was received.
- Only hold the data for as long as there is a business need to do so.
- Ensure that only people who have a genuine business need to see the data will have access to it.
- On receipt, store data received securely
- Move, process and destroy data securely i.e. in line with the principles set out in HM Government [Security Policy Framework](#), issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information.
- Comply with the requirements in the [Security Policy Framework](#), and in particular prepare for and respond to Security Incidents and to report any data losses, wrongful disclosures or breaches of security relating to information. The SRA is certified to ICO 27001 security standard.
- Seek permission from HM Revenue & Customs before onward disclosing information to a third party where disclosure is permitted by law. Inform HM Revenue & Customs before disclosing information to third parties which is required by law to be disclosed.
- Seek permission from HM Revenue & Customs if you are considering offshoring any of the personal data shared under this agreement.
- Mark information assets with the appropriate government security classification and apply the baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile as set out in [Government Security Classifications](#), issued by the Cabinet Office, and as a minimum the top level controls framework provided in the Annex – Security Controls Framework to the GSC.
- The disclosing party also agrees to notify the recipient of:
 - any restrictions on the use to which the information can be put, and
 - any restrictions which apply to the onward disclosure of the information, and

in the absence of such notification, the receiving party may assume that there are no such restrictions (in addition to any restrictions that apply as a matter of law).

16.3 If the SRA adheres to different security standards, please state what these standards are here.

N/A

- The SRA is certified to ICO 27001 security standard.

17. Monitoring and Reviewing and arrangements

17.1 This MoU relates to a regular exchange that must be reviewed annually to assess whether the MoU is still accurate and fit for purpose.

17.2 Reviews outside of the proposed review period can be called by representatives of either participant. Any changes needed as a result of that review must be agreed in writing and appended to this document for inclusion at the formal review date.

17.3 Technical changes necessary to improve the efficiency of the exchange that do not change the overarching purpose can be made without the requirement to review formerly the MoU during its life cycle but must be incorporated at the formal review stage.

17.4 A record of all reviews will be created and retained by each participant.

17.5 Appendix 2 outlines the contacts for amendments to the MoU. Appendix 1 sets out the document control, and the version history of the MoU.

18. Assurance Arrangements

18.1 HM Revenue & Customs has a duty of care to assure any data that is passed on to others. Processes covered by this MoU will be subject to annual reviews, from the date of sign off (to be inserted). HMRC may also choose to introduce ad hoc reviews.

Assurance will be provided by the annual completion of a Certificate of Review & Assurance. The assurance processes should include checking that any information sharing is achieving its objectives (in line with this MoU) and that the security arrangements are appropriate given the risks.

18.2 The SRA agrees to provide HM Revenue & Customs with a signed Certificate of Review & Assurance within the time limits specified upon request.

18.3 The SRA will provide HM Revenue & Customs Internal Audit with sufficient information to conduct assurance reviews of risk management, control effectiveness and governance in respect of this agreement.

19. Security Breaches, Security Incidents or loss or unauthorised disclosure of data

19.1 The designated points of contact (provided at Appendix 2 of this MoU) are responsible for notifying the other participant in writing in the event of loss or unauthorised disclosures of information within 24 hours of becoming aware of the event.

19.2 The designated points of contact will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and notifying the Information Commissioner and the data subjects. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the loss or unauthorised disclosure.

20. Subject Access Requests

20.1 In the event that a Subject Access Request (SAR) is received by either Participant they will issue a formal response on the information that they hold following their internal procedures for responding to the request within the statutory timescales. There is no statutory requirement to re-direct SARs or provide details of the other Participant in the response. However, each Participant will notify the other if a SAR is received in respect of any personal data shared under this agreement. Contact details are at Appendix 2.

20.2 Full details of Data subject's rights in relation to processing of personal information can be found in each Participant's Privacy Notice – links below. Also, see ICO Guidance.

20.3 HMRC

[HMRC Privacy Notice](#)

20.4 SRA

www.sra.org.uk/privacy

20.5 ICO Guidance

[ICO Data Sharing Code of Practice – The rights of individuals](#)

21. Freedom of Information Act (FOI) 2000

21.1 Both participants shall assist and co-operate with each other to enable each organisation to comply with their information disclosure obligations

21.2 In the event of one participant receiving an FOI request that involves disclosing information that has been provided by the other Participant, the organisation in question will notify the other to allow it the opportunity to make representations on the potential impact of disclosure.

21.3 All HMRC FOI requests must be notified to the [Central HMRC FOI Team inbox](#)

21.4 The SRA is not subject to the provisions of the Freedom of Information Act 2000 (FOIA), however, as a transparent regulator the SRA applies its own SRA Transparency Code in a similar way to the FOIA.

21.5 SRA requests for information must be forwarded to the SRA Information Governance team.

22. Issues, disputes, and resolution

22.1 Any issues or disputes that arise as a result of exchange covered by this MoU must be directed to the relevant contact points listed in Appendix 2. Each participant will be responsible for escalating the issue as necessary within their given management structure.

22.2 Where a problem arises it should be reported as soon as possible. Should the problem be of an urgent nature, it must be reported by phone immediately to the designated business as usual contact (listed in Appendix 2) and followed up in writing the same day. If the problem is not of an urgent nature it can be reported in writing within 24 hours of the problem occurring.

23. Costs

23.1 Will there be a charge for this service?

Yes

No

24. Termination

24.1 This MoU may be terminated with immediate effect upon notice by either participant.

24.3 In the event of a significant security breach or other serious breach of the terms of this MoU by either Participant the MoU will be terminated or suspended immediately without notice.

24.4 In the event of a failure to cooperate in a review of this MoU or provide assurance the agreement may be terminated or suspended without notice.

25. Signatories

25.1 Signed on behalf of the HM Revenue & Customs:

I accept the terms of the Memorandum of Understanding on behalf of HM Revenue & Customs.

Signature:	Edwige Hill	
Print Name:	Edwige Hill	
Date:	23/07/2024	
Position:	Deputy Director ISBC Agents & Technical Compliance	
Contact details:	Tel no: 03000 520899	Email: edwige.hill@hmrc.gov.uk

25.2 Signed on behalf of the Solicitors Regulation Authority

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

Signature:	Andrew Turton	
Print Name:	Andrew Turton	
Date:	29/07/2024	
Position:	Director of Risk & Information Governance	
Contact details:	Tel no: 0370 606 2555	Email: Andrew.Turton@sra.org.uk

25.3 Additional Signatories if the agreement is between multiple organisations Check if N/A

I accept the terms of the Memorandum of Understanding on behalf of **[Insert OGD/PSB]**

Signature:		
Print Name:		
Date:	Click or tap to enter a date.	
Position:		
Contact details:	Tel no:	Email:

26. Appendices and Annexes

26.1 Appendix 1 – Document Control

Document Control Personnel

Key Personnel	Organisation	Name	Department
Author	HMRC		
	SRA		
Approver	HMRC		

	SRA		
Review Control	HMRC		
	SRA		

Version history

Version	Date	Summary of changes	Changes Marked
0.1	21/11/2022	Initial Draft	

Review dates

Version	Publication date	Review date

26.2 Appendix 2 – Business Contactsa) Business as Usual Contacts – HMRC






Contact	Email	Responsibility
Tom Moore, ISBC A&TC, Agent Compliance Team	tom.moore@hmrc.gov.uk	Operational Queries
Information Policy & Disclosure	ipd.disclosure (CS&TD TAD)	Legal Issues
Christina Parkinson – Deputy Director, A2, VAT Litigation	christina.parkinson@hmrc.gov.uk	Review and amendments to MoU
Tom Moore	tom.moore@hmrc.gov.uk	Security Incidents
Subject Access Requests to:	SARs, ISBC (ISBC) lc.dpa@hmrc.gov.uk	Subject Access Requests (SAR's)
Solicitors Office and Legal Services – FOI Team	Central HMRC FOI Team inbox	Freedom of Information
HMRC Office of the Data Protection Officer	DPO Office, Mailbox (CSIR DPO)	Advice on data protection issues e.g. GDPR, DPA 2018

b) Business as Usual Contacts – SRA

Contact	Email	Responsibility
Intelligence Unit		Operational Queries

Christopher Hall, Intelligence Manager	christopher.hall@sra.org.uk	
Intelligence Unit	intel@sra.org.uk	Legal Issues
Christopher Hall, Intelligence Manager	christopher.hall@sra.org.uk	
Intelligence Unit	intel@sra.org.uk	Review and amendments to MoU
Christopher Hall, Intelligence Manager	christopher.hall@sra.org.uk	
Information Governance team	srainformationcompliance@sra.org.uk	Security Incidents
Information Governance team	srainformationcompliance@sra.org.uk	Subject Access Requests (SAR's)
Information Governance team	srainformationcompliance@sra.org.uk	Freedom of Information/ requests for information

26.3 Annexes

Annex Ref	Description	Document
Annex A	Glossary of Terms and Abbreviations	 Annex A.docx
Annex B	DCMS Guidance on Controller relationships	 Annex B.doc
Annex C	To be completed when Direct / Brower access is required	 Annex C - Direct Access.docx
Annex D	Instruction on how to add 'Go to TOC' (Table of Contents) button	 Annex D.docx
Annex E	HMRC Internal Processes	 Annex E.pdf