

## **LEDS/HOB Open Space:**

### **LEDS Data Sharing Update Paper**

**v1.0**

**04<sup>th</sup> July 2019**

#### **Discussion Document**

This document has been written with the aim of stimulating discussion on data sharing within Law Enforcement Data Service (LEDS). It is not intended to be viewed as current Home Office policy. It is to be circulated to and viewed only by members of the LEDS Open Space.

### Purpose

1. The purpose of this paper is to provide sight of the approach to the Data Sharing Agreements within LEDS and to promote further discussion.
2. This paper will be discussed in the LEDS Open Space on 17 July 2019. The aim is to provide further information in due course, picking up any concerns raised at the meeting and future developments.

### Summary

This paper has been drafted to provide an update on the Data Sharing Agreement and actions in relation to Data Sharing. The Data Sharing Agreement will be between all LEDS user organisations and will provide clarity about their respective expectations should be and what their obligations and responsibilities are. The annotated skeleton agreement is attached in the Appendix to this document. The outlined plan for this area of work is to have completed the engagements with organisations currently sharing data through the PNC to understand better if there are more proportionate ways of sharing information by October 2019.

### Key questions posed by this paper

1. What additional mechanisms could be considered within the data sharing agreement to protect privacy, whilst promoting appropriate data sharing?
2. The role for the Open Space outlined in Action 123 limits Open Space to scrutinising the proportionality statements in the context of data sharing. Is this appropriate?

### Update on Open Space Actions in relation Data Sharing

**Action 16 – HO committed to providing provocation paper on data sharing in LEDS, including but not limited to the types of data shared and sharing of data with 3rd parties.** The Home Office will now undertake an exercise to understand the proportionality of access to data and data sharing. This will take the form of writing out to each organisation using the PNC. The Home Office will receive from each organisation a necessity and proportionality summary in relation to the data they currently receive. This exercise is not just about seeking to reduce the data available. The organisations will also be asked to comment on data types that they do not currently receive, where they feel it might be appropriate for their work. All responses will be compiled and organised into themes, say, for example, non-constabulary law enforcement, vetting or court processing. The aim will be to compare organisations within themes and produce rationalisations. The following are example questions;

- is one organisation getting access to more data than others performing a similar task?
- is there a reason for this or should there be a levelling up/down for different organisations?
- should different data accesses be created in order to reduce the potential privacy impacts?

The mechanism of access to LEDS data also needs to be considered. Perhaps in more cases in future, some organisations will not be provided electronic access directly into the system. It might be that public sector third-party organisations could play a greater role in answering questions. This will need to be fully impact assessed.

**Action 17 – Further conversations needed on data sharing and data input to LEDS from external sources.**

Details about data from external sources will be disclosed where this does not impact upon operational capabilities. This itemisation will help the conversations on data sharing. This will be informed by the proportionality exercise outlined in the Action above.

**Action 18 - Discussion needed in data sharing conversation on how data is shared, if standards for data quality can be enforced on data from external sources & how this data could get on LEDS.**

Data from external sources will be subject to data quality measures. Those are being developed as part of the Data Quality and Standards project. These standards will be referenced in the Code of Practice and in the Data Sharing Agreement.

**Action 123 - HO to explore role of the Open Space to be involved in the data sharing process.**

The Home Office will conduct the activities in Actions 16, 17 and 18 and complete the Data Types document. The data types document will define what each field of each record should contain and what it means. The LEDS Data Types Policy is the Home Office Policy analysis and advice on future LEDS Data Types, to be used for Policy formation required for LEDS. For each type of record, it will detail; how the data is created, how long it is retained, who the owners of the record are and the reasons for access to that data type. This is with the aim of feeding into an Open Space discussion that;

- Ensures the rationale for data sharing is appropriately explained,
- Inconsistencies are surfaced.

This should ensure that the Open Space has the opportunity to constructively challenge the proportionality and protections for sharing data. It would be difficult to construct a formal role for Open Space in approving the sharing of data but a role in scrutinising the proportionality statements etc would be welcomed.

## Appendix A

### Data Sharing Agreements

#### 1. The Agreement

- The date of the agreement

#### 2. The Parties

- The parties to the agreement will be those listed in Schedule 1<sup>1</sup> of the document and will be revised as necessary if for any reason parties are added or removed.

#### 3. Background

- Sets out the basic<sup>2</sup> reasons for the agreement as to who will share and who will receive personal data and the geographical area covered by the agreement. This will be covered in an attached Schedule.
  - i) The data controller/discloser – agrees to share personal data<sup>3</sup> within its control with the data processor/receiver in the British Islands<sup>4</sup> and Gibraltar under the terms set out in the agreement,
  - ii) The data processor/receiver agrees to use the personal data provided by the data controller/discloser in the geographical location of British Isles under the terms set out in the agreement,
  - iii) This does not include any current or future commercial arrangements entered into by the parties, and
  - iv) Organisations supply data to one of the joint controllers for the use of other joint controllers or processors. Those agreements will be documented within an attached Schedule.

#### 4. Agreed terms

- Rules of Interpretation and definitions used in the agreement are located here. This includes legal powers within which the parties act.
- Controller, Processor, Data Subject, Personal Data, Sensitive Processing, Processing, and Technical and Organisational Measures will have the meanings given to them in the DPA.

#### 5. Purpose of the agreement

- The purpose of the agreement, terms and conditions are set out so that each party is aware of their operational, legal, and ethical responsibilities when they share personal data. It specifies the terms by which personal data is shared, namely for;
  - i) Prevention, investigation and detection of criminal offences;
  - ii) Prosecution of criminal penalties;

---

<sup>1</sup> See Open Space Artefact 1 for a current list of organisations

<sup>2</sup> Detailed purposes for sharing each data type will be included in a schedule. This will include the legal basis under which the data is shared.

<sup>3</sup> Including sensitive personal data.

<sup>4</sup> The British Islands, is England, Wales, Scotland, Northern Ireland, Isle of Man, Jersey, Northern Ireland, Guernsey.

- iii) Safeguarding children and other vulnerable persons from harm, including their economic security;
  - iv) Safeguarding the public and prevention of threats to public security;
  - v) National security
- All parties must abide by the terms of the agreement when providing and processing personal data.
6. Single point of contact
- A single named point of contact must be provided by each party to maintain oversight of their organisation's responsibilities under the agreement. These will be outlined in an attached Schedule.
7. Compliance with National Data Protection Laws
- All United Kingdom parties must abide by the terms of the Data Protection Act 2018 and other relevant legislation, for example, General Data Protection Regulation when providing and processing personal data. United Kingdom Organisations must be registered with the Data Protection Authority in compliance with the legislation unless they are exempt. Details will be set out in the accompanying Schedule.
  - Equivalent standards of protection will apply to Organisations based in Jersey<sup>5</sup>, Gibraltar<sup>6</sup>, Guernsey and Isle of Man. Organisations in those territories will have to comply with GDPR provisions in the same way as if in the UK. Each of these British Territories will have the same standards of notification to their jurisdiction's independent regulator. All data protection regulators will have the ability to exercise audit and oversight this might be in conjunction with the UK regulator. The exact mechanism for that will be determined and shared with the Open Space.
8. Shared Personal Data
- The types of personal data that will be shared include: –
    - i) Those who are suspected and under investigation for a crime
    - ii) Those who have been convicted of an offence
    - iii) Those who are victims of crime
    - iv) Those who are witnesses to crime or another incident
    - v) Those who are being sought after being reported missing or who have gone missing previously
    - vi) Those who are being sought after absconding from lawful detention, failing to attend court or to answer bail, individuals being sought in connection with an investigation
    - vii) Those who are considered vulnerable and to whom a duty of care is owed,
    - viii) Those who are subject to a protection order<sup>7</sup>

---

<sup>5</sup> Jersey, Guernsey and the Isle of Man are outside of the EU but have "adequacy notices" from the European Commission in relation to the standards of data protection existing in these territories. These adequacy notices pre-date the GDPR but are considered current under "grandfathering" rules. Guernsey's re assessment of adequacy is currently being conducted by the European Commission.

<sup>6</sup> Gibraltar will leave the EU at the same time as UK. Her Majesty's Government of Gibraltar is planning to include mechanisms in law for the uninterrupted transfer of personal data between Gibraltar and the UK.

<sup>7</sup> Examples including against Forced Marriage and Female Genital Mutilation (FGM), Slavery and Trafficking Prevention and Risk orders, Non-Molestation Orders and Occupation Orders.

- ix) Those who are subject to restrictions on their liberty<sup>8</sup>
- x) Vehicle keepers
- xi) Licence holders including drivers, alcohol, pharmaceutical and firearms
- xii) Contact details for those reporting an item as lost or stolen
- xiii) A person who is the main contact for a vulnerable person

9. Sensitive personal data

- Certain types of sensitive data may be shared between the parties to the agreement. This might include the following information –
  - i) Racial or ethnic origin
  - ii) Political opinions<sup>9</sup>
  - iii) Religious or philosophical beliefs<sup>10</sup>
  - iv) Trade union membership<sup>11</sup>
  - v) Genetic or biometric data
  - vi) Data concerning health
  - vii) Sex life or orientation
  - viii) Information that identifies a person as a privileged professional such as minister of religion or conscience, journalist, legal counsel or medical practitioner<sup>12</sup>
  - ix) The commission or alleged commission by them of any offence
  - x) Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings
- Details of restrictions will be noted in an accompanying Schedule. All shared personal data must be proportionate and relevant and comply with personal data provisions and ethical practices.

10. Fair and lawful

- All data sharing by all parties must be in accordance with the principles set out in Part 3 of the Data Protection Act 2018, noted in paragraphs of the agreement. Or Part 2 GDPR if this is more appropriate.<sup>13</sup>

11. Processing of shared personal data by the processor

- Shared personal data must be processed in accordance with one of the following legal requirements/principles
  - i) It is carried out to meet certain legal requirements [not just contractual ones];
  - ii) It is carried out to protect the data subject's individual vital interests

---

<sup>8</sup> Examples including against terrorism - Terrorism Prevention and Investigation Measures (TPIMS), Restriction of Liberty Orders in Scotland and Football Banning Orders.

<sup>9</sup> Political opinion is only likely to be held where it is relevant in the context of a criminal investigation or duty of care to protect not as a routine practice. For example, if it was an aggravating factor in an assault.

<sup>10</sup> Religious or philosophical beliefs are only likely to be held where it is relevant in the context of a criminal investigation or duty of care to protect not as a routine practice. For example, the provision of appropriate care in detention.

<sup>11</sup> Trade Union Membership is only likely to be held in the context of a criminal investigation or duty of care to protect.

<sup>12</sup> Information about certain professions will be handled as sensitive to minimise the interference with their privacy and those that interact with them.

<sup>13</sup> As provided for in DPA and GDPR information might be treated under either Part 2 or 3 depending if it is more appropriate to do so.

- iii) It is carried out to protect the public interest or as required in the execution of lawful authority by one/both parties to the agreement
  - iv) It is carried out to meet the legitimate/lawful purposes of one/both parties to the agreement, but this must be both proportionate and necessary to each individual case, and must not affect the individual rights and liberties of the data subject
- Processors must process sensitive data according to the following requirements
    - i) To perform/exercise a legal requirement or obligation imposed by data controller under the employee's contract of employment
    - ii) To protect vital interest of a data subject or a connected person, acting on their behalf if the data subject is unable to provide consent either physically or mentally, or if the data controller is unable to obtain the data subject's consent.
    - iii) To exercise their official functions to protect the public interest and safeguard public security
    - iv) Processing relates to ethnic or racial origin to review any aspects regarding the existence or lack of equal opportunity considerations.
  - When shared personal data is disclosed by each party, the Data controller must ensure privacy notices are clear and transparent to the data subjects.<sup>14</sup> The information provided must allow the data subject to easily understand what personal data is being shared, how it will be stored, reasons it is being shared and to whom it is being provided. Information must be provided to the data subject about the receiving organisation or the identity of the data receiver.

## 12. Data Quality

- The parties have agreed a reliable means of converting Shared Personal Data to ensure compatibility with each party's respective datasets as set out in attached **Error! Reference source not found.**
- Prior to the commencement date the Data Discloser shall ensure, Shared Personal Data are accurate and that procedures are in place for the Data Receiver to sample Shared Personal Data and it will update the same if required prior to transferring the Shared Personal Data.

## 13. Data Subject's rights

- Data Subjects have the right to obtain certain information about the processing of their Personal Data through a Subject Access Request. In circumstances where the processing of an individual's personal data is not in compliance with data protection laws they can request correction, deletion or blocking of their personal data.
- The Parties agree that their respective single points of contact (**SPoCs**) shall be accountable for maintaining a record of access requests that cover Shared Personal Data, the decisions made and any information that was exchanged.

---

<sup>14</sup> Information about who might be subject to processing will be set out in the LEDS DPIA, Code of Practice, language of LEDS all of which will be published. The relationship between these documents will be described in the public guide accompanying the Code of Practice.

The Parties further agree that records shall include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

- The Parties agree to provide reasonable assistance to each other to enable them to comply with Subject Access Requests and respond to any other queries or complaints from Data Subjects.

14. Data Retention and Deletion

- A Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes.
- Parties shall continue to retain Shared Personal Data in accordance with any statutory periods or periods set out in the Information Commissioner's Office (ICO) Data Sharing Code or any other relevant code of practice, including the College of Policing's Authorised Professional Practice (APP) on the Management of Police Information (MoPI).
- Data Disclosers shall ensure that any Shared Personal Data are destroyed in accordance with the agreed Deletion Procedure set out in Schedules
  - i) on termination of the Agreement;
  - ii) on expiry of the Term of the Agreement;
  - iii) once processing of the Data are no longer necessary for the purposes they were originally shared for
- Following the deletion of Shared Personal Data, Data Disclosers shall notify SPoCs that this has been deleted in accordance with the Deletion Procedure in attached Schedule

15. Transfers

- Transfers of personal data shall mean any sharing of personal data by the Data Receiver with a third party, and shall include, but is not limited to, the following:
  - i) storing Shared Personal Data on servers outside the EEA<sup>15</sup>.
  - ii) subcontracting the processing of Shared Personal Data to data processors located outside the EEA.
  - iii) granting third parties located outside the EEA access rights to the Shared Personal Data.
  - iv) transferring personal data to a competent authority outside the EEA.
- A Data Receiver shall not disclose or transfer Shared Personal Data to a third-party data controller located outside the EEA unless it complies with the Provisions of Chapter 5 of the DPA.
- Data transfers of personal data including sensitive personal data will be subject to the operational exigencies established in attached Schedule

---

<sup>15</sup> EEA in this context is written to include the United Kingdom of Great Britain and Northern Ireland and British Territories with an Adequacy Notice determination by the European Commission.

16. Security

- Data Disclosers shall only provide the Shared Personal Data to Data Receivers by using secure methods as agreed and set out in Schedules
- Having regard to the state of technological development and the cost of implementing such measures, the Parties have in place appropriate technical and organisational security measures as set out in the attached Schedule in order to:
  - (a) prevent:
    - (i) unauthorised or unlawful processing of the Shared Personal Data; and
    - (ii) the accidental loss or destruction of, or damage to, the Shared Personal Data
  - (b) ensure a level of security appropriate to:
    - (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
    - (ii) the nature of the Shared Personal Data to be protected.

17. Training

- It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data
- The level, content and regularity of training shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the Shared Personal Data.
- The training materials for LEDS will be developed under the supervision of the College of Policing. There will be updates to the original training materials and it will be the responsibility of each organisation to ensure they are understood and implemented.
- A Schedule to this agreement will cover the minimum Training and Learning standards and review periods.

18. Data security breaches and reporting procedures

- Having considered the applicable national data protection laws and guidance, the parties should have in place their own guidance that must be followed in the event of a **Data Security Breach**. This also applies to any breaches of Security which compromise the Security of the Shared Personal data.
- Parties will notify any potential or actual losses of the Shared Personal Data to all SPoCs as soon as possible and, in any event, within 1 Business Day of identification of any potential or actual loss to enable the Parties to consider what action is required in order to resolve the issue.
- The Parties agree to provide reasonable assistance to facilitate the handling of any Data Security breach in a timely manner. Detailed processing included in attached Schedule.

19. Review and termination of agreement.

- As per the LEDS Code of Practice, any additional Data Receiver that wishes to be part of this agreement shall complete and submit a data sharing request form, as set out in attached schedules. This request form will be circulated to all Parties. The additional party will be included into this Agreement subject to objection from any Party to be communicated between the Parties in writing.

- Parties shall review the effectiveness of this agreement every 12 months. The Parties shall continue, amend or terminate the Agreement depending on the outcome of such review. Each SPoC will be invited to participate in the review.
- The review of the effectiveness of the data sharing initiative will involve:
  - (i) Assessing whether the purposes for which the Shared Personal Data is being processed are still compliant with this Agreement;
  - (ii) Assessing whether the Shared Personal Data is still as listed in the schedules.
  - (iii) Assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and
- Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS) will inspect Parties' arrangements for the processing of Shared Personal Data.

20. Resolution of disputes with data subjects or the data protection authorities

- In the event of a dispute or claim brought by a data subject or the Data Protection Authority, that Party will inform the others about any such disputes or claims, and all parties agree to cooperate with a view to settling them amicably in a timely fashion.
- The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or the Data Protection Authority. If they do participate in the proceedings, they may do so remotely by any electronic means. The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- Each Party shall abide by a decision of a competent court of the Data Discloser's country of establishment or of the Data Protection Authority which is final and against which no further appeal is possible.

21. Warranties

- Each Party will:
  - (i) Process the Shared Personal Data in compliance with all instruments that apply to its personal data processing operations.
  - (ii) Make available to the Data Subjects who are third party beneficiaries a copy of this Agreement, unless the Clause contains confidential information.
  - (iii) Respond within a reasonable time to enquiries from the relevant Data Protection Authority in relation to the Shared Personal Data.
  - (iv) Respond to Subject Access Requests in accordance with the Privacy and Data Protection Requirements.
  - (v) Where applicable, maintain registration with all relevant Data Protection Authorities to process all Shared Personal Data for the Agreed Purpose.
  - (vi) Take all appropriate steps to ensure compliance with the security measures set out in the Connections Contract.

- Each Data Discloser warrants and undertakes that it will ensure that the Shared Personal Data are accurate.<sup>16</sup>
- The Data Receiver will not disclose or transfer the Shared Personal Data to a third-party data controller located outside the EEA<sup>17</sup> unless it complies with the obligations set out in this agreement.
- Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

22. Indemnities

- The Parties undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Agreement, except to the extent that any such liability is excluded in this agreement.
- Indemnification hereunder is contingent upon
  - (i) the party(ies) to be indemnified (the **indemnified party(ies)**) promptly notifying the other party(ies) (the **indemnifying party(ies)**) of a claim,
  - (ii) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and
  - (iii) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.

23. Allocation of cost

- Each Party shall perform its obligations under this Agreement at its own cost.

24. Limitation of liability

- No Party excludes or limits liability to the other Parties for:
  - (i) fraud or fraudulent misrepresentation;
  - (ii) death or personal injury caused by negligence;
  - (iii) a breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
  - (iv) any matter for which it would be unlawful for the parties to exclude liability.
- Subject to clause 22, no Party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:
  - (i) any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;
  - (ii) loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or
  - (iii) any loss or liability (whether direct or indirect) under or in relation to any other contract.

25. Third party rights

---

<sup>16</sup> The Data Quality Dashboards and Code of Practice will indicate where standards exist

<sup>17</sup> EEA again includes countries with adequacy notices from the European Commission

- Except as expressly provided in (data subjects rights) a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.
- No one other than a party to this Agreement shall have any right to enforce any of its terms.

26. Variation

- No variation of this Agreement shall be effective unless it is in writing and agreed by the Parties (or their authorised representatives).

27. Waiver

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

28. Severance

- If any part of this Agreement is or becomes invalid, illegal or unenforceable, it shall be amended to the minimum extent necessary to make it so. If modification is not possible, the relevant part shall be deemed deleted. Any change under this clause shall not affect the validity and enforceability of the rest of this agreement.
- If any part of this Agreement is invalid, illegal or unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended result of the original provision.

29. Changes to the applicable law

- In case the law changes so that this Agreement is no longer adequate, the Parties agree that the SPoCs will negotiate in good faith to review the Agreement in light of the new legislation.

30. No partnership or agency

- Nothing in this agreement is intended to establish any partnership or joint venture between the parties, constitute any Party to make or enter into any commitments for or on behalf of any other Party
- Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

31. Further assurance

- At its own expense, each Party shall, reasonably try and deliver documents and perform acts that may reasonably be required for the purpose of giving effect to this Agreement.

32. Force majeure

- No Party shall be in breach of this Agreement if delay or failure are from events or circumstances beyond its reasonable control. In such circumstances the Party shall be entitled to a reasonable extension of the time.

33. Rights and remedies

- The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

34. Notice

- Any notice or other communication given to a Party under or in connection with this agreement shall be in writing, addressed to the SPoCs and shall be:
  - (i) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
  - (ii) sent by email to the SPoC.
- Any notice or communication shall be deemed to have been received:
  - (i) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address;
  - (ii) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service.
  - (iii) if sent by email, at 9.00 am on the next Business Day after transmission.
- This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

35. Counterparts

- This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.
- Where Schedules are varied (by agreement of the Parties) to include a new Party, that new Party shall execute a new counterpart of this Agreement. Once executed, that new counterpart shall be incorporated into and form part of the one Agreement.

36. Governing law

- This Agreement shall be governed by and construed in accordance with the law of England and Wales.

37. Jurisdiction

- Jurisdiction will need to be fully determined:
  - It will include the law enforcement organisations within 4 nations of the United Kingdom; England, Northern Ireland, Scotland and Wales. It will also include the British Crown Dependencies comprising the Bailiwick of Guernsey, Bailiwick of Jersey and the Isle of Man and the

British Overseas Territory of Gibraltar. For this agreement this area will be known as the domestic sphere.

- As some law enforcement operations are at least in part international, it will be in effect for law enforcement operations and purposes; wholly in the domestic sphere, partly in the domestic sphere or elsewhere.

### Draft list of Schedules

- Schedule 1 Parties to this agreement
- Schedule 2 Detailed purposes for sharing data including legislative basis and whether under Part 2 or Part 3 GDPR.
- Legal basis and legal quality,
  - Pressing social aim,
  - Necessity, and
  - Proportionality
- Schedule 3 Data supplied to one Joint Controllers for the use of other Controllers or Processors
- Schedule 4 SPoC duties
- Maintaining a record of Data Subject Access Requests
  - Maintaining a record of bulk data taken from LEDS and stored or processed elsewhere
  - Maintaining deletion records
  - Maintenance of training, learning and qualification records
  - Notify any potential or actual losses of the Shared Personal Data to other SPoCs
  - Annual review of the effectiveness of this agreement
  - Liaison with HMICFRS over inspections or follow ups
  - Review this agreement in the light of new legislation
- Schedule 5 Data Protection registration details of all Organisations and how to raise a complaint
- Schedule 6 Restrictions on the sharing of data
- Schedule 7 Data Quality arrangements, where to find them and how to apply them
- Schedule 8 Deletion Protocols
- In accordance with Data Sharing Codes, MoPI and College APP as appropriate
  - Mechanisms for deletions
  - Process for bulk record deletion
- Schedule 9 Transfers overseas for operational exigencies
- Law Enforcement Agencies transfer data overseas at the request of and in partnership with international law enforcement agencies. This schedule will include a statement on the considerations.
- Schedule 10 Security
- Governance & Information Risk Return (GIRR) process,
    - How it is applied and to who?

**17072019 LEDS/HOB Open Space Data Sharing Discussion Paper**

Schedule 11 Training standards required to access, maintain or oversee LEDS

Schedule 12 Data security breach processes

Schedule 13 Data Sharing Request forms to access additional data or for access to LEDS