**Data Sharing Agreement – Name of DSA**

| **Summary of purpose** | |
| --- | --- |
|  | |
| **Parties** | |
| * xx * xx * xx | * xx * xx * xx |
| Controller to Controller / Joint Controllers [delete unnecessary options) | |

| **Part 2 processing** [delete unnecessary options] | **Part 3 processing** [delete unnecessary options] |
| --- | --- |
| Personal data | Personal data |
| Special category data | Sensitive data |
| Criminal data | Pseudonymised data |
| Pseudonymised data | Anonymised/Aggregate data |
| Anonymised/Aggregate data |  |
| **Key legislation titles** (full details in appendices) | |
| * xx * xx * xx * xx | * xx * xx * xx * xx |

| **Publish date** |  | **Review date** |  | **Termination Date** (N/A if ongoing) |  |
| --- | --- | --- | --- | --- | --- |

**Contents**

[**1. The Data Sharing Agreement 4**](#_heading=h.1fob9te)

[**1.1. Ownership of this agreement 4**](#_heading=h.3znysh7)

[1.2. Parties to this agreement 4](#_heading=h.tyjcwt)

[1.2.1 Local Partners 4](#_heading=h.3dy6vkm)

[**1.3. Responsibilities of parties involved 4**](#_heading=h.1t3h5sf)

[**1.4. Review and termination 5**](#_heading=h.4d34og8)

[**2. Purpose and Benefits 5**](#_heading=h.2s8eyo1)

[**2.1. Purpose 5**](#_heading=h.17dp8vu)

[2.1.1 Serious Violence Duty this section can be removed if the SVD doesn’t apply 5](#_heading=h.3rdcrjn)

[**2.2. Benefits 6**](#_heading=h.26in1rg)

[2.3. Data Protection Impact Assessment (DPIA) 7](#_heading=h.lnxbz9)

[**2.4. Lawful Basis 7**](#_heading=h.35nkun2)

[2.4.1 Part 2 processing 7](#_heading=h.1ksv4uv)

[2.4.2 Part 3 processing for law enforcement purposes 9](#_heading=h.44sinio)

[2.4.3 Consent 10](#_heading=h.2jxsxqh)

[2.4.4 Vital interests 10](#_heading=h.2jxsxqh)

[2.4.5 Applicable legislation 10](#_heading=h.2jxsxqh)

[**2.5. Proportionality and necessity 10**](#_heading=h.z337ya)

[**2.6. Other relevant legislation 11**](#_heading=h.3j2qqm3)

[2.6.1 Common law duty of confidence 11](#_heading=h.1y810tw)

[2.6.2 Freedom of information 12](#_heading=h.4i7ojhp)

[**3. Individuals 12**](#_heading=h.4i7ojhp)

[**3.1. Data subject rights requests and complaints 12**](#_heading=h.2xcytpi)

[**3.2. Data subjects 14**](#_heading=h.1ci93xb)

[3.3. Deceased individuals 14](#_heading=h.3whwml4)

[**4. Data 14**](#_heading=h.2bn6wsx)

[**4.1. The data to be shared 15**](#_heading=h.3as4poj)

[4.1.1 Personal data 15](#_heading=h.3tbugp1)

[4.1.2 Special category data 16](#_heading=h.1pxezwc)

[4.1.3 Criminal data 16](#_heading=h.2p2csry)

[**4.2. Storing and handling information securely 16**](#_heading=h.147n2zr)

[**4.3. Outside UK processing 17**](#_heading=h.23ckvvd)

[**4.4. Data quality 17**](#_heading=h.ihv636)

[**4.5. Data breaches/incidents 17**](#_heading=h.32hioqz)

[**4.6. Retention and Disposal 18**](#_heading=h.1hmsyys)

[4.6.1 Retention periods 18](#_heading=h.41mghml)

[4.6.2 When sharing ends 18](#_heading=h.2grqrue)

[**5. Appendices 19**](#_heading=h.vx1227)

[**5.1. Appendix A: Parties to this agreement 19**](#_heading=h.3fwokq0)

[**5.2. Appendix B: Applicable legislation 21**](#_heading=h.4f1mdlm)

[5.3. Appendix C: Defence for sharing data 22](#_heading=h.2u6wntf)

[5.4. Appendix D: Security of data 23](#_heading=h.19c6y18)

# The Data Sharing Agreement

## Ownership of this agreement

This agreement was drafted under the Pan-London Data Sharing Project by a working group of selected representatives from the parties to the agreement, facilitated by LOTI (London Office of Technology and Innovation) at London Councils. Parties to this agreement cannot amend it, or add appendices, unless agreed as part of a formal review. Operational documents and processes will sit under this DSA.

## Parties to this agreement

The parties are registered data controllers under data protection legislation and are listed in **Appendix A**. This agreement covers data sharing that is Controller to Controller between Joint Controllers [delete unnecessary option].

A signatory from each party will agree to sharing under this DSA on the [Information Sharing Gateway](https://www.informationsharinggateway.org.uk/Default.aspx) (ISG). [ISG is expected but delete this sentence if another route is agreed]

### Local Partners

The parties to this DSA may employ or work with other data controllers specific to their organisation or borough eg a local charity, or NHS Trust employed to deliver a local authority service. These local partners may be involved in sharing data under this DSA. As the local partners change at different times, it is not possible to make them a party to the DSA when it is published to the Information Sharing Gateway. Instead, the parties must seek agreement from their relevant local partners to this DSA, and document this.

## Responsibilities of parties involved

All parties will

* comply with data protection legislation and the responsibilities within this DSA, according to their statutory and professional duties.
* choose a suitable signatory, who has the authority to commit to the responsibilities.
* suitably vet staff through any necessary employee checks, including advanced checking such as through the Disclosure & Barring Service (DBS).
* have appropriate written contracts or agreements with employees, agency staff, volunteers, and anyone with access to the personal data. These must include requirements for compliance with policies which include confidentiality and secure handling of personal data.
* communicate this DSA to staff and instruct them to contact their organisation’s Data Protection Officer/Lead if they are unsure at any point about the sharing of personal data.
* help staff to understand their responsibilities, for example by directing them to the:
  + [ICO Data Sharing Checklist](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/#:~:text=Check%20whether%20the%20sharing%20is%20justified&text=%E2%98%90%20What%20is%20the%20sharing,the%20issue%20you%20are%20addressing%3F)
  + [ICO 10 step guide to sharing information to safeguard children](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/)
* share this DSA with any relevant local partners and document their agreement to it.

## Review and termination

| **Publish date** |  | **Review date** |  | **Termination Date** (N/A if ongoing) |  |
| --- | --- | --- | --- | --- | --- |

This DSA will be reviewed through the Pan-London Data Sharing Project, unless otherwise agreed by the parties’ Data Protection Officers. The review will ensure the purposes are still relevant, the scope has not changed, the benefits to the data subjects and organisations are being realised, and the procedures for data security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the parties.

A party becomes a data controller when they receive personal data shared under this DSA and may continue to process this data when this DSA ends, where the party has documented a lawful basis to do so.

# Purpose and Benefits

## Purpose

[Describe the purpose(s) for each party]

### Serious Violence Duty [this section should be removed if the SVD doesn’t apply]

The Serious Violence Duty (SVD) in the Police, Crime, Sentencing and Courts Act 2022 requires local partnerships to complete a Strategic Needs Assessment (SNA) to understand how violence is affecting their communities, and design a response through a Violence Reduction Strategy. Under the SVD there are specific limitations under section 16 and 17 of the PCSC Act on the disclosure of information by health and social care authorities. Patient information and personal information (ie information that can be used to identify a person either directly or indirectly) is not permitted to be disclosed and health and social authorities can only share anonymous data.

| **Specified Authorities** defined in section 11 of, and Schedule 1 to, the PCSC Act | **Relevant Authorities (defined within the PCSC Act)** who are able to cooperate with the specified authorities as necessary |
| --- | --- |
| Local authorities | Education authorities |
| Probation Service | Youth Custody authorities |
| Fire & Rescue services | Prison authorities |
| Police | An organisation or person described in s10 of the PCSC Act |
| Integrated Health Boards |  |
| Local Health Boards |  |
| Youth Offending Teams |  |

Preventing violence and its root causes can improve the health and wellbeing of individuals and communities and have wider positive implications for the economy and society. Violence is a major cause of ill health and poor wellbeing and is strongly related to inequalities. Interventions, especially those in early childhood, can stop people from developing a propensity for violence, and improve educational outcomes, employment prospects and long-term health outcomes.

Where a party wishes to use personal data, special category data, personal data relating to criminal convictions and offences, and personal data processed for law enforcement purposes shared under this DSA for meeting responsibilities under the SVD, it must ensure that it justifies the use and necessary, lawful and proportionate to do so.

The SVD is separate from the existing powers to share data under the Crime & Disorder Act 1998 section 115.

## Benefits

**Individuals**

[Suggestions to be expanded]

* receipt of better-tailored services
* improved wellbeing
* improved support to treat substance misuse

**Parties** (name the relevant party and the benefit)

[Suggestions to be expanded]

* more effective use of resources
* ability to plan use of resources
* ability to deliver statutory duties

**Society**

[Suggestions to be expanded]

* more effective use of resources
* reduction in crime or fear of crime
* reduced cost for treating substance misuse

## Data Protection Impact Assessment (DPIA)

Each party is responsible for undertaking a DPIA where it considers it necessary.

The working group that drafted this DSA completed a DPIA. Parties may use that DPIA in its entirety, adapt it to fit that party’s template and risk tolerances, use their own process and template, or not undertake a DPIA.

## Lawful Basis

Each party’s lawful basis for the sharing of the data under this DSA is listed below. All parties agree that they have an appropriate policy document in place when processing special category data or personal data relating to criminal convictions and offences.

### Part 2 processing

For processing personal data the UK GDPR lists lawful basis conditions in Article 6 (personal data) and Article 9 (special category data) that must be identified to cover the processing. Part 2 of the Data Protection Act 2018 (DPA 2018) covers general processing. When processing special category data, a condition from Schedule 1 Part 1, or Schedule 1 Part 2 of the DPA 2018 must be identified.

Article 10 of the UK GDPR applies when processing data relating to criminal convictions and offences, and a condition from the DPA 2018 Schedule 1 Part 3 must be identified.

The conditions relevant to this DSA are:

| **Article 6 lawful basis conditions** [delete unnecessary options] | **Applicable party** | |
| --- | --- | --- |
| c) legal obligation |  |
| e) performance of a task carried out in the public interest |  |
| f) purposes of the legitimate interests |  |

| **Article 9 lawful basis conditions** [delete unnecessary options or whole table if inapplicable] | | **Applicable party** | |
| --- | --- | --- | --- |
| f) necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |  | |
| g) substantial public interest |  | |
| h) purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services |  | |
| i) public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices |  | |
| j) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |  | |

| **Article 9(2) (b) (h) (i) (j) - Sch 1 Pt 1** [delete unnecessary options or whole table if inapplicable] | **Applicable party** | |
| --- | --- | --- |
| Employment, social security and social protection |  |
| Health or social care |  |
| Public health |  |
| Research |  |

| **Article 9(2) (g) - Sch 1 Pt 2** [delete unnecessary options or whole table if inapplicable] | **Applicable party** | |
| --- | --- | --- |
| Statutory & government purposes |  |
| Equality of opportunity or treatment |  |
| Preventing or detecting unlawful acts |  |
| Regulatory for unlawful acts and dishonesty |  |
| Preventing fraud |  |
| Safeguarding of children and individuals at risk |  |
| Administration of justice |  |
| Racial/ethnic diversity at senior management |  |
| Protecting the public against dishonesty |  |
| Terrorist financing or money laundering |  |
| Support for individuals with disability or medical condition |  |
| Safeguarding economic well-being |  |

| **Personal data relating to criminal convictions and offences.- Sch 1 Pt 3** [delete unnecessary options or whole table if inapplicable] | **Applicable party** | |
| --- | --- | --- |
| Legal claims |  |
| Accounts for child indecency offences |  |
| Judicial acts |  |
| Extension of Sch 1 Pt 2 |  |

### Part 3 processing for law enforcement purposes [delete this section if inapplicable]

The DPA 2018 covers processing for law enforcement purposes in Part 3. The law enforcement purposes are defined in Section 31 as “prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

Processing must be carried out by a ‘competent authority’, which is defined in Section 30, with reference to Schedule 7.

| Competent authority name(s) | Purposes |
| --- | --- |
|  |  |

There are additional safeguards required for ‘sensitive processing’. This is defined in Section 35(8) as:

1. the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
2. the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
3. the processing of data concerning health;
4. the processing of data concerning an individual’s sex life or sexual orientation.

One of either Section 35(4) or (5) must apply. Both require an appropriate policy document to be in place.

Section 35(4) requires the consent of the data subject, which is not generally used by parties to this agreement, and 35(5) requires that the processing be ‘strictly necessary’ for the law enforcement purposes, and meets a condition in Schedule 8. The competent authorities that are party to this DSA consider the data sharing to be ‘strictly necessary’ and do not consider that there are less intrusive means of obtaining personal data held by partners.

| **Sch 8 Law enforcement conditions** [delete unnecessary options or whole table if inapplicable] | **Applicable party** | |
| --- | --- | --- |
| Statutory purposes |  |
| Judicial acts |  |
| Legal claims |  |
| Archiving |  |
| Administration of justice |  |
| Safeguarding of children and individuals at risk |  |
| Preventing fraud |  |

### Applicable legislation

The parties have legislation, statutory guidance, and public duties for processing personal data that justifies the lawful basis conditions identified above. These are listed in **Appendix B***.*

## Proportionality and necessity

[Describe how you decided on the minimum amount of the data necessary to achieve your purpose.]

## Other relevant legislation

The disclosure of any personal data to achieve the objectives listed in this DSA must consider the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence.

### Common law duty of confidence [delete this section if inapplicable]

A duty of confidence arises where it is reasonable for a data subject to expect that the information will be kept confidential. The duty can be overridden by legislation or justifiable necessity, or where consent has been provided by the data subject.

While much of the personal data processed under this DSA is considered confidential, it is considered that data subjects will expect the parties to share personal data for the purposes of safeguarding and wellbeing, preventing harm, and the prevention and detection of crime.

**Override for duty of confidentiality** [delete unnecessary options]

* Not applicable
* Implied consent
* Explicit consent
* Section 251 support (this means you have support from the Secretary of State for Health and Care or the Health Research Authority)
* Legal requirement (law that requires data sharing. [State the legal requirement]
* Overriding public interest (eg to prevent or detect a serious crime or to prevent serious harm to another person, balanced against the public interest in maintaining public confidence in public sector organisations. [State the justification]

# Individuals

## Data subject rights requests and complaints

The data subject rights and how each party complies with them are listed in **Appendix C**.

**Rectification, erasure or restriction**

If an individual successfully requests the erasure or limitation of use of their data, the relevant party will communicate this to the other parties where appropriate. Each party is responsible for securely disposing of such information or limiting its processing.

**Complaints**

The parties will [Describe how complaints will be handled **-** by individual parties or where one or more parties have responsibility on behalf of others]

## Data subjects

Parties to this agreement are in positions of power over data subjects and individual data subjects have little or no control over why and how their data is processed. Many of the data subjects are vulnerable.

**Types of data subjects** [add text to specifically explain the data subjects and delete unnecessary options]

| Customers, service users, clients or residents | Licence and permit holders |
| --- | --- |
| Service provider/contractor staff | Employees |
| Patients | Witnesses |
| Complainants and enquirers | Victim/complainant of crime |
| Carers/Guardians/Family/Support network/Next of Kin | Actual or suspected offenders or perpetrators |
| People in images in photographs, film, body worn/dashcam footage, CCTV, or audio recordings | Advisers, consultants and professional experts eg doctor, social worker, police officer, lawyer |
| Visitors | Volunteers |
| Traders or people subject to inspection | Councillors, MPs, elected officials |
| Students | Supporters or group members |

## Deceased individuals

The sharing may involve data of deceased persons which will not be covered by data protection legislation, but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

# Data

## Data categories

[Delete unnecessary options]

| **Part 2 processing** | **Part 3 processing** |
| --- | --- |
| Personal data | Personal data |
| Special category data | Sensitive data |
| Personal data relating to criminal convictions and offences | Pseudonymised data |
| Pseudonymised data | Anonymised/Aggregate data |
| Anonymised/Aggregate data |  |

| **Describe any anonymisation or pseudonymisation of data or outputs** - for pseudonymised data include details of which organisation holds the key to re-identification |
| --- |
|  |

## The data to be shared

For agreements involving personal data being shared by the MPS, specific guidance to MPS officers/staff on appropriate datasets will be provided within Appendix D.

The types of personal data to be shared are listed below.

### Personal data [delete unnecessary options]

| **Type of data** | **Describe the data** - are there datasets or named reports? Is there any data specifically excluded? |
| --- | --- |
| Name |  |
| Address |  |
| Contact details (phone/email) |  |
| Postcode |  |
| Partial postcode |  |
| DOB |  |
| Age |  |
| Gender |  |
| Financial information incl pension records |  |
| Property information |  |
| Family / relationship information incl next of kin |  |
| Location data eg GPS or IP address |  |
| NHS number |  |
| Any unique reference number |  |
| Other (describe below) |  |
| Social care information |  |
| Human Resources information |  |
| Employment |  |
| Social media names and activity |  |
| Education information |  |
| GP (or other medical professional) contact details |  |
| Support network |  |
| Housing information |  |
| Legal or personal representative incl Power of Attorney |  |
| Images in photographs, film, body worn/dashcam footage, CCTV, or audio recordings |  |
| Referral / Assessment information |  |
| Referees |  |
| Copies of ID like passport or driving licence |  |
| Physical description |  |

### Special category data [delete unnecessary options]

The types of personal data to be shared are listed below.

| **Type of data** | **Describe the data** - are there datasets or named reports? Is there any data specifically excluded? |
| --- | --- |
| Information relating to an individual’s physical or mental health or condition |  |
| Biometric information to uniquely identify an individual eg facial recognition |  |
| Genetic data eg a DNA sample |  |
| Information relating to an individual’s sexual life or sexual orientation |  |
| Racial or ethnic origin |  |
| Political opinions |  |
| Religious or philosophical beliefs |  |
| Trade union membership |  |

### Personal data relating to criminal convictions and offences [delete this section if inapplicable]

Personal data relating to criminal convictions and offences is shared under this DSA. The data is [describe the data].

## Storing and handling information securely

[Describe the following as relevant: data format; location of data; data flows (attach images if available); roles and access and access controls.]

[Describe the data security standards and which party has responsibility, whether for data they hold or data within a shared system or database - this should include reference to encryption, password protection, role based access controls (RBAC), restricted physical access, business continuity plans and security policies.]

## Outside UK processing [delete this section if inapplicable]

[Describe any outside UK processing]

| **Applicable party** | **Describe** |
| --- | --- |
|  |  |

## Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality.

Any party learning of the inaccuracy of personal data is responsible for promptly informing the parties with whom that data has been shared.

**[Describe how data quality and accuracy will be checked and assured** - will you use standardised formats, how will you check the accuracy of data matching, which party is responsible?]

## Data breaches and incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches and cyber security incidents which impact the confidentiality, integrity or accessibility of data.

If the incident may impact the processing of another party to this DSA, all relevant parties should be informed as soon as possible, with all relevant parties agreeing to the appropriate coordination of the incident. The decision to report the incident will lie with the data controller(s) of the information. The parties agree to provide all reasonable assistance to each other, at their own expense, to facilitate the handling of any personal data incident.

Each party has internal disciplinary procedures that cover security breaches (including misuse or unauthorised disclosure). If misuse is found, each party has a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

**[Describe how incidents will be handled** - which party is responsible (if not all individually), is one party responsible for a system or database?]

## Retention and Disposal

The parties may have different retention periods, potentially with a different period for combined data.

Each party will state a retention period and securely dispose of or delete personal data once it is no longer required.

### Retention periods

The following retention periods apply to the data shared under this DSA. These may be for the data each party is sharing and/or for the combined data being shared.

| **Data** | **Organisation** | **Retention period** | **Automated or manual deletion? What processes ensure that disposal happens at the allotted time?** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### When sharing ends

The parties must agree what happens to the shared data once the data sharing activity ends.

| **Data** | **Organisation** | **End of sharing activity** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendices

## Appendix A: Parties to this agreement

| **Organisation name or type** | **Duties** | **Part 3 competent authority for this DSA?** |
| --- | --- | --- |
| Metropolitan Police | * The prevention and detection of crime * The maintenance of the King’s peace * Protection of the vulnerable |  |
| London Borough  (state all or name each borough involved) | * Co-ordinates, gathers, processes, risk assesses and shares information held about all the areas covered in the DSA in conjunction with information received from partner agencies, to enable the council to undertake its statutory duties in these areas * Makes decisions on whether to undertake enforcement or other appropriate actions under its powers in the legislation listed in this DSA * Allocates resources in accordance with priority of tasks and policies * Co-ordinates, gathers, processes, risk assesses and shares information covering all the areas under this DSA with partners to achieve common goals * Undertakes interventions as necessary to ensure the safeguarding of vulnerable people * Decides whether to undertake prosecutions when offences covered by the legislation in this DSA has been breached and it is within the council’s remit * Takes appropriate and proportionate steps to ensure the safety of employees and others |  |
| Probation Service | * The Probation Service is a statutory criminal justice service that supervises high-risk offenders released into the community. |  |

## 

## Appendix B: Applicable legislation

State the relevant sections and describe the duties and how the legislation applies to the listed party.

| **Legislation/Statutory guidance** | **Party to which it applies** | **Main purpose of Legislation** | **How it applies to this data sharing** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Appendix C: Data subject rights

[Add rows as necessary to describe the approaches of the different parties to the DSA.]

| **Individual right** | **Party or type of party** | | **How the parties complies (or state not applicable if the right does not apply)** |
| --- | --- | --- | --- |
| **The right to be informed** about the collection and use of personal data – privacy information. |  | |  |
| **The right of access** to details of data use and to receive a copy of their personal data, commonly called a subject access request. |  | |  |
| **The right to rectification** to have inaccurate personal data rectified or completed if it is incomplete. |  | |  |
| **The right to erasure**  (Does not apply when using the lawful basis conditions of Article 6: legal obligation, public task or legal claims, or Article 9: health and care services, public health or archiving, research or statistical purposes.) |  | |  |
| **The right to restrict processing**  and limit how their data is used. | Does not apply to this DSA. | | |
| **The right to data portability** to obtain and re-use their personal data. | Does not apply to this DSA. | | |
| **The right to object** to the use and sharing of personal data where the parties are using the public interest or legitimate interests conditions It is unlikely that an objection would be upheld but each request must be considered on a case-by-case basis. |  |  | |

## 

**5.4 – Appendix D : Detailed guidance on appropriate data sets for MPS Officers**

**Scenario 1 -** Monthly Multi-agency Meeting

**Data subject/Data** – Suspect / Name, address, dob, relevant criminal history

**Data Subject/Data** – Victim / Name, address, dob, relevant health data

**Means of sharing** – Via Box prior to meeting

**Relevant recipients** – Local Authority. Not appropriate for voluntary Agency

**Notes:** …..

**Scenario 2 -** Immediate safeguarding concern

**Data subject/Data** – Suspect / Name, address, dob, relevant criminal history

**Data Subject/Data** – Victim / Name, address, dob, relevant health data

**Means of sharing** – Merlin report – sent via encrypted email to ….

**Recipient –** Local Authority Safeguarding Team

**Notes:** …..

Sharing of data beyond that stipulated above will need to be justified on case-by-case basis