Data/Information Sharing Agreement – Integrated Offender Management

Contents

1. Introduction to the Data Sharing Agreement

This Data Sharing Agreement [DSA] documents how the parties to this agreement, will share information between themselves about offenders to reduce reoffending and to protect the public from harm. Specifically to:

- Identify suitable offenders for IOM management.
- Effectively manage selected offenders:
  - Identify criminogenic needs and address them together.
  - Provide effective joint enforcement.
  - Monitor and provide a suitable level of multi-agency supervision and track progress towards exit.

The key agencies are listed in Appendix A, and the agreement is to be signed by all relevant parties, including local partners, voluntary sector, and any specialist organisations.

By signing this Agreement, the named agencies agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal Data to be shared.
- Set out the lawful basis condition under UK GDPR and Data Protection Act 2018 through which the information is shared, including reference to the Human Rights Act 1998 and the Common Law Duty of Confidentiality.
- Stipulate the roles and procedure that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

Parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

1.1. Ownership of this agreement

This agreement was drafted by a working group of representatives of the police, health, local authorities and London Councils. These professionals were specialists in safeguarding, social work, police procedures, information governance and law. The local authority representatives worked under the banner of the Information Governance for London Group (IGfL), to draft one agreement that would work for all boroughs, CCGs and police BCUs across London. The aim is to reduce the number of versions of sharing agreements that historically differed between boroughs, partly to reduce the burden on pan-London organisations, that must have agreements with multiple boroughs.

IGfL, a group of information and security professionals at London boroughs, assisted with co-ordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the listed data controllers.

1.2. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act. Signatories are identified as those who have signed this agreement on the platform on which this agreement is hosted (expected to be the Information Sharing Gateway). A list of expected types of signatories is at Appendix A.

All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights & complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.
- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.3. Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks (BPSS or equivalent), DBS, Security Vetting or Counter Terrorist Check [CTC].

1.4. Assessment and review

A review of this information sharing agreement will take place initially after six months and then annually thereafter, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and organisations are being realised, and the procedures followed for information 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 signatory parties.

The working group who drafted this agreement strongly recommend that a working group approach is used for any reviews, as this was a successful way to achieve pan-London and cross-specialism consensus to one sharing agreement.

1.5. Termination of agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are data controller.

2. Purpose and Benefits

To provide an effective IOM scheme within the Borough to reduce reoffending and protect the public from harm.

The information shared using this agreement will allow partners to provide the best range of services to IOM clients, whilst addressing any continuing offending or anti-social behaviour.

2.1. Benefits

2.2. Principles of information sharing

Effective information sharing is a vital element of both early intervention and safeguarding of children and young people at risk of harm or neglect. Organisations can hold different piecThe benefits of this DSA are to:

- Cover the sharing of information for Integrated Offender Management purposes.

- Remove barriers to effective information sharing.
- Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations.
- Identify the correct lawful basis to share personal information.
- Ensure information is shared whenever there is a requirement to do so.
- Enables authorities to share data on performance, quality assurance, learning and impact analysis.
- Raises awareness amongst all agencies of the key issues relating to information sharing and gives confidence in the process of sharing information with others.
- Greater efficiencies in processes and resources.
- Reduction in crime, the likelihood of being a victim of crime and the fear of crime
- Reduction in the costs of crime
- Enhanced public confidence in the Criminal Justice Services through an integrated approach to the management of offenders
- Safer communities

es of information which need to be placed together to enable a thorough assessment and plan to be made.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such as Working Together to Safeguard Children 2018 or the Children and Families Act 2014, which places responsibilities on organisations outside of the Partnership such as sports clubs, private organisations, and the voluntary, community and faith sectors.

The sharing of personal data must comply with both the GDPR Principles and the Caldicott Principles, listed at Appendix B. Together, those principles lead to a series of questions and considerations to be answered before sharing takes place. These are listed as an Information Sharing Checklist in *Appendix D: Information Sharing Checklist.*

2.3. Lawful Basis

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area and each Partner must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian.

For purposes other than law enforcement by competent authorities

Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

Article 6 (1) – Personal Data Processing
(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject

(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller Use of this article requires that the Data Protection Act section 8 be satisfied. The laws given at *Appendix C – Applicable legislation* provide for each party a legal basis under section 8 – the specifics are noted in the appendix.

Article 9 (2) – Special Category Personal Data Processing
(c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject Use of this article requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are: ● *Statutory etc., and government purposes under Para 6(1)(2)* ● *Preventing and detecting unlawful acts under Para 10(1)(2)(3)* ● *Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)*
(h) **provision of health or social care** - processing is necessary for the 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 Use of this article requires that the Data Protection Act Section 10(2) be satisfied. This requires that a condition within Schedule 1, Part 1 is met. For this agreement these are: ● *Health or Social Care Purposes under Para 2 with appropriate safeguards as required by section 11(1) of the act and Article 9(3) of the UK GDPR*

Article. 10 : Processing of personal data relating to criminal convictions and offences
Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.
Data Protection Act 2018 Schedule 1 *PART 1 Health or social care purposes* *2(1) This condition is met if the processing is necessary for health or social care purposes.* *(e)the provision of social care* *PART 2 SUBSTANTIAL PUBLIC INTEREST CONDITIONS* *Requirement for an appropriate policy document when relying on conditions in this Part.* *5(1)Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).* *(2) See also the additional safeguards in Part 4 of this Schedule.* *Statutory etc and government purposes*

6(1) This condition is met if the processing—
(a)is necessary for a purpose listed in sub-paragraph (2), and
(b)is necessary for reasons of substantial public interest.
(2) Those purposes are—
(a)the exercise of a function conferred on a person by an enactment or rule of law;
Preventing or detecting unlawful acts

10(1) This condition is met if the processing—
(a)is necessary for the purposes of the prevention or detection of an unlawful act,
(b)must be carried out without the consent of the data subject so as not to prejudice those purposes, and
(c)is necessary for reasons of substantial public interest.

For the purposes of law enforcement by competent authorities

The "competent authorities" are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are generally (but not exclusively) police, probation services, youth offending teams and government departments.

The "law enforcement" purposes are defined in Section 31 of the DPA 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".*

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

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

The additional requirements are given in Section 35(4) and (5). Both require an appropriate policy document, and this document will form part of the policy for such processing, although competent authorities will need to satisfy themselves their own internal policy documents fully cover such use.

Section 35(4) requires the consent of the data subject, 35(5) requires that the processing be strictly necessary for the law enforcement purposes and meets a condition in Schedule 8.

For the processing in relation to the purposes here, the following conditions in Schedule 8 are met:

- Statutory etc. purposes Para 1(a)(b);
- Administration of justice Para 2;
- Protecting individual's vital interests Para 3;
- Safeguarding of children and of individuals at risk Para 4(1)(2)(3)(4);

The applicable legislation that provides the lawful basis is listed in more detail in *Appendix C – Applicable legislation.*

2.4. Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not generally the lawful basis the public sector organisations use for processing information shared under this agreement. It is possible that the other parties, such as voluntary groups, may use consent as lawful basis for some personal data processing. Each party is responsible for managing consent where they use consent as the lawful basis condition.

2.5. Proportionality and necessity

Proportionality and necessity are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not and apply their professional judgement.

You are expected to justify that you believed sharing was necessary for one of the following criteria:

- necessary for the purposes of preventing or detecting crime
- required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
- in the particular circumstances, was justified as being in the public interest.

Or that you acted in the reasonable belief that:

- the person had a legal right to do the obtaining, disclosing, procuring or retaining
- the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it

2.6. Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must also be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott Principles also apply to all information sharing and they are listed in Appendix B: Data Protection & Caldicott Principles.

- Human Rights Act 1998 (HRA)
- Common law duty of confidentiality
- Confidentiality and Sharing for Direct Care

2.7. Common Law Duty of Confidence

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children.

However, for the police, as a safeguard before any information is passed on, it will undergo an assessment check against criteria (included in Child Abuse Investigation Command Standard Operating Procedures) by the Public Protection Desk (PPD). Whilst still applying proportionality and necessity to the decision, the protection of children or other vulnerable persons would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim.

Information held by other agencies that will be may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure as information can be shared where consent has been provided or where there is a strong enough public interest to do so.

When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

2.8. Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply, and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who holds the information (data controller).

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

3.1. Right to be informed – Privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UKGDPR and will issue appropriate notices which inform the data subject that the information will be shared with the parties under this agreement.

In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

3.2. Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of organisation concerned.

3.3. Data subjects

There is a breadth of data subjects whose data is shared under this agreement. The data subjects include the following:

- child
- family members, carers and other persons whose presence and/or relationship with the child, is relevant to identifying and assessing the risks to that child
- victims
- actual or suspected perpetrators
- professional adviser or consultant (eg doctor, lawyer)
- professional opinions of employees eg social workers and police officers
- witnesses
- people captured on CCTV or similar

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

4. Data

The personal data and its processing involved in these workstreams is extensive, highly sensitive and at times intrusive. There is a high volume of data and data subjects.

Anonymisation or pseudonymisation will rarely be possible because of the way the work focusses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Information will include:

- **Personal, special category and criminal data** to enable the swift and effective safeguarding of children and improved safeguarding provision in the borough
- **Personal, special category and criminal data** for law enforcement purposes, including data defined as **sensitive data** for the competent authorities for law enforcement purposes
- **Aggregated (anonymised or pseudonymised) data** reporting to enable the partnership to further understand the safeguarding priorities.
- **Aggregated (anonymised or pseudonymised) and personal data** regarding employees in relation to serious case reviews, investigations into allegations against staff, learning review and workforce development.
- **Personal and anonymised data** required for statutory returns.

4.1. The data to be shared

Due to the complexity of the work involved in the subject of this DSA, providing a prescriptive list of data fields to be shared is difficult. Not all the above information will be shared in every case; only relevant information will be shared on a case-by-case basis where an organisation has a 'need-to-know' the information.

Data that will be shared includes:

- name and contact details
- age/date of birth
- ethnic origin, religion and other equalities information
- physical descriptions
- criminal information on allegations and convictions, police information and intelligence, information from the London Fire Brigade, anti-social behaviour (ASB) data
- IOM specific reoffending performance data (Home Office ID-IOM system)
- school and educational information
- health records including NHS number, GP, London Ambulance Service and other
- information on sex life and sexual orientation
- housing information
- probation service data
- social services information, referrals and assessments
- opinions of employees in educational establishments and voluntary/3rd sector
- whether the offender is already known to other services and third sector/voluntary
- financial information

- images in photographs, film or CCTV
- employment information
- Details of incidents and encounters that relate to criminogenic needs including those that affect safeguarding, risk and vulnerability (redacted if required).
- Vulnerable Persons reports (MERLIN in London)
- Details of incidents or encounters that relate to offending and offending behaviour (redacted if required).
    - Convictions / offending history (PNC data)
    - Crime reports (CRIS in London)
    - Custody record (NSPIS in London)
    - Criminal Intelligence reports (Crimint in London)
    - ASB reports (Airspace in London).

4.2. Deceased persons

It is noted that the sharing may involve data of deceased persons. This data 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.

4.3. Confidential information

In this agreement, we refer to personal data, as defined by data protection legislation. However, the word 'confidential' may be used by individuals and practitioners to describe information and can mean different things to different people.

Confidential can mean:

- Personal and special category data as defined by data protection legislation
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings
- Information which is not already lawfully in the public domain or readily available from another public source
- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

4.4. Storing and handling information securely

Information should only be stored and shared in accordance with data protection legislation and follow information security policies and procedures of the relevant organisation.

Information should always be shared securely, either by a secure IT connection, encrypted email, secure sharing platform, or secure and tracked transfer of paper documents. Information should never be sent via a non-secure method. Special category data may need a higher level of security. The employee/organisation sending the information must choose the most appropriate method of transfer and be responsible for its safe delivery. Organisations will have secure data repository and sharing platforms, such as MS Teams, Google, FTP sites and E-CINS. To use these, the parties must establish

that these are suitably secure, and that access is only provided to those who need it, and only to the data needed.

Email is not generally a secure method of transferring personal data. Although two or more of the parties may have additional encryption that allows for an encrypted path between two of the parties, this cannot be identified simply from the email address. It would be prudent for parties to establish whether there are any encrypted paths between them, and write that into the organisation's processes for employees.

In the absence of that, secure email systems such as CJSM, Egress and Encrypt and Send must be used. Description of specific transfer processes must be in relevant process documents within each organisation.

Information may be shared over the phone, in a virtual meeting, or a face to face meetings. Employees must ensure that attendance and distribution of content is limited, with minutes or recordings with limited distribution. Sharing by telephone should be avoided unless the requirement is urgent, and email is not practicable.

Any paper records printed must be kept to a minimum and kept secure at all times whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.5. Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted.

Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.

4.6. Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data.

4.7. 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 informing the parties with whom that data has been shared.

4.8. Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UKGDPR, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed, and appropriate co-ordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.9. Retention & Disposal

Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.

Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.

5. Signatures

This agreement is signed on behalf of:

The Metropolitan Police

Name and Rank

Cmdr [redacted], Head of Profession for Criminal Justice

[redacted]

Date

24th November 2021

Local Authorities:

Signatories will be managed through publication of this agreement onto the Information Sharing Gateway

Version control	
Document production date	February 2021
Document currency	Final Version October 2021

6. Appendix A – Parties to this agreement

Organisation	Duties
London Borough Councils	● Community Safety Partnership decides local priority in terms of addressing local problems ● Co-ordinates local services to run effective IOM partnership ● Mobilises all local resources/services in reducing re-offending through the IOM programme
Metropolitan Police Service, British Transport Police & City of London Police	● Co-ordinates, gathers, processes, risk assesses and shares police information relevant to Public Protection, Missing Children, CSE, Child Protection (MERLIN reports) • Supports assessments of risk and vulnerability
Probation Service	• Co-ordinates, gathers, processes, risk assesses and shares Probation information relevant to adult offenders • Supports assessments of risk & vulnerability
Local health partner	● Co-ordinates, gathers, processes, risk assesses and shares health information relevant to the child or young person • Supports assessment of risk and vulnerability • Identifies opportunities for early help, joint assessments and interventions
DWP / Job Centre Plus	• Co-ordinates, gathers, processes, risk assesses and shares information regarding families in receipt of benefits • Advises on eligibility for accessing benefits • Supports assessments of risk and vulnerability.
Local CCG	• Co-ordinates, gathers, processes, risk assesses and shares health information relevant to midwifery, ante-natal, health visiting, school nursing, specialist health services, GPs • Supports assessments of risk & vulnerability
Local substance misuse partner	• Co-ordinates, gathers, processes, risk assesses and shares drug and alcohol service information relevant to adults and young people • Supports assessment of risk and vulnerability Identifies opportunities for early help, joint assessments and interventions
London Ambulance Service	• Gathers and shares information relating to the treatment, transportation and relevant medical information of individuals. • Provides emergency transportation, urgent care and support to the health service • Supports assessments of risk and vulnerability

Housing ALMO/Partnership	Co-ordinates, gathers, processes, risk assesses and shares housing applicants, tenant and leaseholder's information relevant to children and adults • Advises on eligibility for accessing accommodation under the homeless legislation and Housing Allocation Scheme
Other relevant Vol Orgs/Agencies	Co-ordinates, gathers, processes, risk assesses and shares information relevant to adults and young people service users • Supports assessment of risk and vulnerability Identifies opportunities for early help, joint assessments and interventions

7. Appendix B: Data Protection & Caldicott Principles

The Principles as described in Article 5 of the General Data Protection Regulation.

1) Fair & Lawful
processed lawfully, fairly and in a transparent manner in relation to the data subject

2) Purpose limitation
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3) Data minimisation
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4) Accuracy
accurate and, where necessary, kept up to date; Inaccurate data must be erased or rectified without delay

5) Storage limitation
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6) Integrity & Confidentiality
secured through appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7) Accountability
processed by organisations that take responsibility for the personal data, with appropriate measures and records in place to demonstrate compliance.

The Caldicott Principles

Principle 1
Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2
Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3
Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4
Access to confidential information should be on a strict need -to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5
Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6
Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7
The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8
Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. As a minimum, this should include providing accessible, relevant and appropriate information. In some cases, greater engagement will be required.

8. Appendix C – Applicable legislation

Legislation	Main purpose of Legislation
The Mental Health Act 1983[1] and the Mental Health Act Code of Practice[2]	The Code of Practice provides statutory guidance to registered medical practitioners, approved clinicians, managers and staff of providers, and approved mental health professionals on how they should carry out functions under the Mental Health Act in practice. The act was substantially revised by the 2007 act but remains the key legislation. This regulation provides specific powers for dealing with mental health issues giving a legal basis under Section 8 of the DPA for this use. It specifically excludes learning disability, alcohol or drug dependence.
The Local Government Act 2000[3]	The main principles of the Local Government Act 2000 are to give powers to local authorities to promote economic, social and environmental well-being within their boundaries. This was mostly replaced by the Localism Act 2011 below, but still applies in Wales.
The Localism Act 2011[4]	The Localism Act created general powers for Local Government to act as an individual for any purpose, with specific goals to promote economic, social and environmental well-being within their boundaries. This regulation provides the general power for local authorities to act in any manner they believe suitable for the purposes giving a legal basis under Section 8 of the DPA for this use. However, as a general power it can be challenged, and an additional legal basis is preferred.
The Education Act 2002[5]	The Education Act 2002 puts a duty on schools to exercise their functions with a view to safeguarding and promoting the welfare of children. All schools are required by law to teach a broad and balanced curriculum which promotes the spiritual, moral and cultural development of pupils and prepares them for the opportunities, responsibilities and experiences of life. This regulation provides specific powers for dealing with school-related safeguarding and welfare issues giving a legal basis under Section 8 of the DPA for this use.
The Children Act 1989	Under S.47 of the *Children's Act 1989*, a Local Authority has a duty to investigate when informed that a child in their area is in police protection or the subject of a protection order. This regulation provides specific powers giving a legal basis under Section 8 of the DPA for this use.
The Children Act 2004	Under Sections 10 and 11 of the *Children Act 2004*, the police, local authorities and primary care trusts must co-operate with other relevant partners to safeguard and

[1] https://www.legislation.gov.uk/ukpga/1983/20/contents
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435512/MHA_Code_of_Practice.
[3] http://www.legislation.gov.uk/ukpga/2000/22/contents
[4] https://www.legislation.gov.uk/ukpga/2011/20/contents
[5] http://www.legislation.gov.uk/ukpga/2002/32/contents

	promote the welfare of children and ensure that arrangements are made to improve the wellbeing of children in their area. This regulation provides a general safeguarding and welfare power giving a legal basis under Section 8 of the DPA for this use
The Children and Families Act 2014	The Act is designed to fully reform services for vulnerable children, by giving them greater protection, paying special attention to those with additional needs, and also helping parents and the family as a whole.
The Criminal Justice Act 2003[6]	This act amended a wide range of provisions in the PACE act and provided new regulations on offence management, disclosure and trials. The regulation clarifies process and procedure for police and their legal basis for use.
The Police and Criminal Evidence Act 1984	This act makes the specific provision for the secretary of state to issue codes of practice to police with statutory effects. It provides the basis for many of the police actions in respect of matters relating to safeguarding and other matters, and as such provides their legal basis for use.
The Children & Social Work Act 2017[7]	The Children and Social Work Act 2017 (the Act) is intended to improve support for looked after children and care leavers, promote the welfare and safeguarding of children, and make provisions about the regulation of social workers. The Act sets out corporate parenting principles for the council as a whole to be the best parent it can be to children in its care. These are largely a collation of existing duties local authorities have towards looked after children and those leaving care.
The Mental Capacity Act 2005[8]	The Mental Capacity Act (MCA) 2005 promotes a person centred approach which promotes autonomy and for those who may lack mental capacity ensures that decisions made on their behalf are made in their best interests and with the least possible restriction of freedoms
The Health and Social Care Act 2012[9]	This act provides for the delivery of Health and Social Care, providing a legal basis for many of the services delivered by parties to this agreement. In particular, it places (section 251B) a duty to share information relating to health and adult social care unless the data subject has specifically objected. This regulation provides a specific duty giving a legal basis under Section 8 of the DPA for this use.
The Crime and Disorder Act 1998[10]	Each LA in England & Wales has the responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.
The Offender Management Act 2007	An Act to make provision about the provision of probation services, prisons and other matters relating to the management of offenders; and for connected purposes.
The Criminal Justice and Courts Service Act 2000	An Act to establish a National Probation Service for England and Wales and a Children and Family Court Advisory and Support Service; to make further provision for the protection of children; to make further provision about dealing with persons suspected of, charged with or

[6] http://www.legislation.gov.uk/ukpga/2003/44/contents
[7] http://www.legislation.gov.uk/ukpga/2017/16/contents
[8] http://www.legislation.gov.uk/ukpga/2005/9/contents
[9] https://www.legislation.gov.uk/ukpga/2012/7/contents
[10] http://www.legislation.gov.uk/ukpga/1998/37/contents

	convicted of offences; to amend the law relating to access to information held under Part III of the Road Traffic Act 1988; and for connected purposes.
Data Protection Act 2018 and UK GDPR	The Data Protection Act 2018 and UK GDPR control how personal information is used by organisations, businesses or central and local government.

9. Appendix D: Information Sharing Checklist

The following questions must be considered when deciding whether to share information.

- Whose information is this?
- Is there a lawful basis to share the information? Justify the purpose and identify relevant legislation that applies.
- Can information be pseudonymised or anonymised ahead of sharing?
- How have individuals been informed that the information will be shared eg via a privacy notice? Will they have the expectation that their information will be shared? Consider whether notifying the individual of the sharing may place someone at risk or prejudice a police or safeguarding investigation.
- Have any requests not to share been received and considered?
- How much information is it necessary to share in this situation?
- Is the information accurate and up to date? Has the difference between fact and opinion been stated?
- Is access to the information limited to only those who need it? Is it being given to the right person?
- Is the information being shared in a secure way?
- Has the decision to share or not share, and the rationale for the decision, been recorded?

Appendix E: Meeting Confidentiality Statement

This statement (or a locally agreed substitute) will be read out at the beginning of each meeting. All attendees must comply, or identify to the Chair before the meeting begins if they are unable to comply, and why. The Chair will take the decision of whether the attendees can continue within the meeting.

The Chair of the Meeting reminds all attendees of the requirements and protocols within the Integrated Offender Management (IOM) Data Sharing Agreement.

The purpose of this meeting is for the relevant agencies to share information/data about offenders between themselves for the purpose of making, modifying and implementing plans to reduce reoffending and to protect the public from harm. The responsibility to take appropriate actions rests with the individual agencies. This includes responsibilities for the sharing of information under this agreement.

All individuals who are discussed at the meeting will be treated fairly, with respect and without discrimination. All work at the meeting will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability, and by the duty to protect the confidentiality of the personal data of the individuals discussed.

Information discussed within the meeting is confidential and must not be disclosed to third parties unless they are a signatory to the IOM Data Sharing Agreement, or when it has been agreed by the partners at the meeting.

Hard copies of information brought to or received at the meeting will be left in the meeting room, where the IOM Co-ordinator is responsible for secure disposal. All agencies must ensure that the minutes are retained securely in line with the agency's retention schedule.

Date of Meeting: _____

By signing the attendance sheet agency representatives agree to abide by this agreement.

Name	Job Title	Organisation
