Information Sharing Agreement (ISA)

Between

Bexley Safeguarding Adults Board:

- **London Borough of Bexley,**
- **SE Borough Command Unit,**
- **Bexley Clinical Commissioning Group, &**
- **Other relevant partners**

Purpose of the ISA: To Safeguard Adults at Risk within the London Borough of Bexley

Freedom of Information Act Publication Scheme	
Protective Marking	BSAB01
Publication Scheme Y/N	Yes
Title	Information Sharing Agreement (ISA) between Bexley Safeguarding Adults Board: • London Borough of Bexley, • SE Borough Command Unit, • Bexley Clinical Commissioning Group, & • Other relevant partners
Version	Version 1
Summary	An agreement to formalise information sharing arrangements between Bexley Safeguarding Adults Board: • London Borough of Bexley, • SE Borough Command Unit, • Bexley Clinical Commissioning Group, & • Other relevant partners For the purpose of Safeguarding Adults within the London Borough of Bexley.
(B)OCU or Unit, Directorate	South East BCU
Author	BSAB Partners amended ADSS Version
Review Date	March 2019
Date Issued	1 May 2018

INDEX

FOREWORD

The Care Act 2014 statutory guidance advises that the first priority should always be to ensure the safety and well-being of the adult at risk

The guidance also states that all organisations must have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and the SAB

The Act puts adult safeguarding on a statutory footing and requires each Local Authority to set up a Safeguarding Adults Board (SAB) with core membership from the Local Authority, the Police, and the NHS (specifically the local Clinical Commissioning Group/s). The SAB has the power to include other relevant bodies.

One of the key functions of the SAB is to ensure that the policies and procedures governing adult safeguarding are fit for purpose and can be translated into effective adult safeguarding practice.

Safeguarding adults at risk is a complex area of work that involves a number of professional organisations working together with the common purpose of preventing or reducing the risk of significant harm to adults at risk from abuse or other types of exploitation, whilst supporting individuals to maintain control over their lives. This includes being able to make choices without coercion. To achieve this, the sharing of information amongst professional organisations who work with vulnerable adults is essential. Early sharing of information is the key to providing an effective response where there are emerging concerns. Sometimes it is only once information from a range of sources is co-ordinated that an adult is identified as being at risk. **It is better that information is shared rather than withheld if this may prevent a vulnerable adult from suffering harm.**

By signing up to this agreement the relevant partner organisations (signatories) are recognising that working together and sharing information effectively is imperative to safeguard those that are at risk or pose a risk to themselves or another, and to prevent, detect and prosecute offences against adults at risk. **This agreement formalises the processes and principles for sharing information between each other, with other professionals and the SAB and any other relevant parties.**

Statement from Independent Chairperson:
I would like to take the opportunity to acknowledge progress in preventing adult abuse and in responding appropriately when it happens. Particularly making progress in sharing information our learning and to make structural, policy and practice improvements.

We will continue to support each other with all our colleagues to acknowledge invaluable work, continue to support and to challenge each other to improve services to Adults in Bexley.

Annie Callanan, Independent Chair, Bexley Safeguarding Adults Board (BSAB)

If you are concerned that an adult you know may be at risk of abuse, harm or neglect from either an individual or an organisation, please make contact with the Safeguarding Adults Team by calling 020 8303 7777.

Section 1 - The Purpose of the Information Agreement

1.1 This Agreement -

- forms the basis for the lawful exchange of information between signatory organisations involved in adult safeguarding

- puts in place arrangements which set out clearly the processes and the principles for sharing information

- sets out the basis upon which requests for information will be made by the signatory organisations involved in adult safeguarding, and how those requests will be dealt with by the signatories

- provides a framework for the secure transfer and confidential sharing of information between signatories

- describes the roles and structures that will support the exchange of information between partners, and security procedures necessary to ensure compliance with responsibilities under the Data Protection Act/General Data Protection Regulation 2018 (GDPR), Caldicott Principles and partner specific security requirements

- will ensure that the Metropolitan Police Service will in addition adhere to requirements of the Guidance on the Management of Police Information (MoPI) and the Authorised Professional Practice (APP)

- describes how this arrangement will be monitored and reviewed with the recommendation being 6 months initially and annually thereafter

- summarises the signatories' legal obligations in relation to information sharing

- does **not** create an absolute obligation to share information: it will not be a breach of the agreement for a signatory to refuse to share information where disclosure of such would constitute a breach of legal or professional obligations owed by that signatory in respect of that information

- does not override the lawful bases available for processing personal data and special categories of data under Data Protection/GDPR or any subsequent Act which may follow

1.2 Scope of this Information Sharing Agreement

The signatories to this agreement are the following agencies/bodies:

1. Bexley Safeguarding Adult Board Partners
    a. London Borough of Bexley Chief Executive
    b. Metropolitan Police Service SE BCU - Tri-Borough Commander
    c. Bexley Clinical Commissioning Group

This agreement **does** cover the sharing and assessing of partner information by:

- London Borough of Bexley High Risk Panel if set up after the date of this Agreement
- A multi-agency group that is not a High Risk Panel and which relates to an adult with care needs; including MASH/MARAC/MAPPA

This agreement **does not** cover the sharing and processing of Partner information where a safeguarding concern does not exist. These activities are covered by separate information sharing agreements / policies.

1.3 Information Sharing in the Context of a Safeguarding Adults Enquiry

1.3.1 Safeguarding Adults Enquiry

The Care Act 2014 says that the duty to undertake a safeguarding adults enquiry arises where a Local Authority has reasonable cause to suspect that an adult in its area (whether or not ordinarily resident there)

- has needs for care and support (whether or not the authority is meeting any of those needs)
- is experiencing, or is at risk of, abuse neglect and
- as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

An adult that any signatory suspects may fall into the above categories will be referred to in this agreement as an “Adult at Risk”.

The Care Act 2014 guidance states that early sharing of information is the key to providing an effective response where there are emerging concerns for an Adult at Risk, and no professional should assume that someone else will pass on information which they think may be critical to the safety and wellbeing of the adult. If concerns are raised about the adult's welfare, whether this be the belief that they are suffering or likely to suffer abuse or neglect, and/or are a risk to themselves or another, information should be shared with the local authority and/or the police if they believe or suspect that a crime has been committed or that the individual is immediately at risk.

Explanations of the type of abuse and criminal offences that Adults at Risk may become victims of, are listed in Appendix B. This is not an exhaustive list.

In the majority of cases the response to a safeguarding enquiry will involve other agencies, for example, a safeguarding enquiry may result in referrals to the police, a change of accommodation, or action by CQC. Where a number of professional organisations are involved in a combined plan, it is recommended that the Local Authority should seek to establish a 'lead' agency for the monitoring and assurance of the plan. Information sharing should be rapid and seek to minimise bureaucracy.

1.3.2 The National Standards

The Association of Directors of Adult Social Services (ADSS) has published a National Standards document in conjunction with key partners including the National Police Chiefs Council (NPCC). This framework is intended to consolidate the experience to date and to further the development of 'Safeguarding Adults at Risk' work throughout England. The implementation of the eleven good practices (Standards) in every local area will lead to the development of consistent, high quality adult protection work across the country. (See Appendix C for a headline copy of the National Standard Framework).

This agreement has been produced in compliance with the National Standard Framework, and the signing of this agreement will help the signatories comply with the Framework in particular Standards 1, 4 and 8. It has been recognised that a number of agencies may be involved in different aspects of the care and support of an adult at risk and this agreement will contribute to achieving the aims of building strong multi-agency partnerships at a local level with agreed working practices in response to instances of abuse and neglect.

By effective information sharing and drawing upon partners specialist skill sets, all partners to this agreement can offer the best possible service to safeguard adults at risks and make a positive impact on public protection.

1.3.3 Assessments and Investigation Strategies

It is key that the adult at risk is involved from the outset in any investigation strategies (unless doing so would put them at greater risk of harm). Family, friends and other relevant people who are not implicated in any crime have an important part to play especially if the person lacks capacity. In these cases, the friends or family should be consulted in line with the Mental Capacity Act 2005. The role of agency representatives, their duties and powers will be governed by the relationship of the person that has caused the harm to the adult at risk.

Staff and volunteers should be aware of the London Multi Agency Safeguarding Policy and Procedures (2015) and be aware of issues regarding abuse, neglect or exploitation. The document recognises variance in terminology between agencies regarding adults at risk who may be considered as vulnerable, and that the terms vulnerable adult and adult at risk are used interchangeably.

Managers of organisations have a key role in the management and coordination of information in response to a Safeguarding Adult Concern.

1.4 Types of Information to be Shared through this Agreement

The types of information likely to be required to be shared include the following.
Due to the complexity and uniqueness of each situation, it is difficult to provide an exhaustive list of what information will be shared but as a minimum the following information should be considered.

1.4.1 Personal Information about Individuals Considered to be a Risk to an Adult at Risk

Personal information needs to be shared to allow relevant agencies to identify these individuals and explain why they are a risk to vulnerable adults. Examples of the kind of personal & sensitive personal data that may be shared include:

- Personal identifiers (names, addresses, dates of birth)
- Current photograph of the offender (if appropriate)
- Descriptive information (photographs, marks, scars; including pressure ulcers)
- Relevant warning markers (e.g. Violence, Drugs, Mental Health, Weapons)
- Reason why they are considered to be a risk
- Details of relevant criminal convictions and non-conviction information
- Relationship with the adult at risk

1.4.2 Personal Information about Adults at Risk

- Name of subject (Adult at Risk) and other family members, their carers and other persons whose presence and/or relationship with the subject, is relevant to identifying and assessing the risks to that vulnerable adult

- Age/date of birth of subject and other family members, carers, other details including addresses and telephone numbers
- Ethnic origin
- Description of incident and police action

1.4.3 Personal information Disclosed about Third Parties may Include:

- Adult at risk relevant family members
- GP who is the primary record holder for all individuals registered with them - where relevant and known
- Employer - where necessary and known

Relevant results from police checks on **relevant** family members mentioned within police databases, or persons such as a general practitioner or an employer again where relevant. This information will only be considered on a case by case basis and is not a blanket for sharing on everybody associated with an adult who is at risk. Information shared on these individuals must be necessary to assist in services and only the minimum required.

Information considered for sharing in regards to associated individuals can include but is not limited to personal identifiers, relationship to the adult at risk and information and or intelligence held by partners that are **relevant** to assisting partners in services or duties towards the adult at risk concerned.

This information may need to be shared to ensure to allow agencies to fully understand the risks posed to/by the individual and stop them from being a victim, repeat victim, suspect or risk to themselves, and *to ensure that all relevant avenues for assistance are considered.*

Section 2 - Description of Arrangements including Security Matters

2.1 General Principles

All information exchanges between the signatories to this agreement must be:

- In accordance with the law;
- Relevant to actions undertaken to safeguard adults;
- Sufficiently detailed for the specified purpose and reasonably accurate;
- Shared in a secure manner; and
- Information exchanged must be used only for the purposes for which it was shared.

Signatories to this Agreement must have regard to the Caldicott Principles -

2.2 The Caldicott Principles

The Caldicott Committee's 1997 *Report* ***on the review of patient-identifiable information***[1] established 6 principles for sharing information, recognising that confidential patient information may need to be disclosed in the best interests of the patient. It also discusses in what circumstances this may be appropriate and what safeguards need to be observed. This report was reviewed in 2013 adding a 7th principle.

The principles are that the **use of information** should be:

1) Justified
2) Necessary
3) Minimal
4) On a need to know basis

and that **users of information** should:

5) Understand their responsibilities
6) Comply with the law

And additionally that

7) The duty to share information can be as important as protecting patient confidentiality.

Principles of confidentiality designed to safeguard and promote the interests of service users and patients should not be confused with those designed to protect the management interests of an organization. These have a legitimate role but must never be allowed to conflict with the interests of service users and patients. If it appears to an employee or person in a similar role that such confidentiality rules may be operating against the interests of Adults at Risk then a duty arises to make full disclosure in the public interest.

2.3 Security Classification

The information shared through this agreement will be marked in accordance with the Government Security Classification (GSC) and information to be shared will not exceed the level "Official Sensitive". For example, information must not be shared if:

- Cause substantial distress to individuals
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on disclosure of information (except the Data Protection Act 1998)
- Disadvantage government or Partners in commercial or policy negotiations with others

[1] Report on the review of patient-identifiable information, Caldicott Committee, 1997, http://www.wales.nhs.uk/sites3/Documents/950/DH_4068404.pdf

2.4 Accuracy of Information

If information held is found to be inaccurate, the agency producing the information will be notified. The producing agency will be responsible for correcting this information, and notifying other recipients of this information of the inaccuracy and the correction. The other recipients will then be responsible for relevant information in their possession being corrected.

2.5 How the Information will be processed

2.5.1 The sharing of information between partner organisations may be proactive or as a result of a request for information. Partner agencies will inform the police about Adults at Risk where a crime may have been committed and police will notify Safeguarding Adults Services and the relevant Health Trust about adults at risk of abuse or neglect, and/or experiencing abuse or neglect, and individuals who pose a risk to Adults at Risk.

Requests will include an explanation as to why the information is necessary and they will be considered on a case by case basis by the signatories.

2.5.2 Where it has come to the MPS's attention that an Adult at Risk is in circumstances that are adversely impacting upon their welfare or safety and/or they are a risk to themselves or others, as well as a crime or intelligence report being created, the reporting officer will create an 'Adult Coming to Notice' (ACN) MERLIN report.

This report will be viewed by **South East BCU** police Public Protection Desk (PPD) / Multi Agency Safeguarding Hub (MASH) contact. If deemed appropriate and necessary to do so to protect and safe-guard the adult at risk, they will share the ACN on to **London Borough of Bexley** relevant partnership team via the secure email link within MERLIN.

2.5.3 If the **London Borough of Bexley** relevant partnership team have concerns about an adult, or if the criteria of Section 42 Care Act 2014 are met the Local Authority must make or cause others to make whatever enquiries it thinks necessary. Any requests from the Local Authority to partner agencies must be in a written format and for police information on a Form 87V. Requests to any partner asking for information will include reasons why they require any information held. In the case of requests to police, the completed form will be sent to the Borough PPD, MASH or Borough Mental Health Liaison Officer (BMHLO). For criminal investigations, partner agencies should initially liaise with the police officer in charge of the enquiry. (Form 87V can be found in Appendix E).

2.5.4 The PPD or designated borough unit will search the appropriate MPS databases and also national police systems for relevant information. The designated unit will consider the information gathered and decide whether it is proportionate, relevant and necessary to be disclosed for the purpose requested.

2..5.5 Any partner refusal to share information under Section 42 Care Act 2014 must be in writing, and for police the original request Form 87V will be returned to the authorising manager. The reply will include an explanation as to why the request did not fall within the defined categories.

2.5.6 In the case of a request to the police, if it is decided that it is proportionate and necessary to disclose information, then the results of the search of MPS and police systems will be collated within an Adult Come to Notice report (on MERLIN) and/or a CRIMINT relating to that request. After removing where necessary any information that is not appropriate to be shared from each report, the police unit will send the finalised answer in the format of Form 87VA back to the requesting agency via the secure email link in MERLIN

or other agreed secure email address listed in section 2.6 of this agreement. (Form 87VA can be found in Appendix D)

2.5.7 Should a meeting be called to discuss a case, a Confidentiality Statement shall be signed by all attending parties. A sample Confidentiality Statement and Register can be found in Appendix F.

2.5.8 Permission must be sought by the partner agencies from the relevant partner for the sharing of information outside of their respective domain. Such permission will only be granted where proposed sharing of relevant and proportionate information is within the agreed principles: i.e. for policing purposes, which includes safeguarding an Adult at Risk. All requests made should be done so by either secure e-mail or in writing so that an audit trail exists.

2.6 Critical Request for Information

A case will be considered 'Critical' if there is immediate risk of harm to the subject or others and information needs to be provided immediately to protect individuals e.g. hostage situations, acts of terrorism, serious attempt by the individual to take their own life etc. The process in these circumstances will vary as stated below.

2.6.1 Initial contact for Critical enquiries will be made to the relevant person listed in the Contacts List found in Appendix G. In the event that the relevant person can not be contacted a locally agreed escalation policy should be followed.

2.6.2 Upon initiating a Critical enquiry the following detail will be requested:

- Requestor's full name, job title, phone number.
- Verification that the case is genuinely 'critical' (i.e. there is immediate risk of harm to the subject or others and information needs to be provided immediately to protect individuals)
- A check that the telephone number provided is the number provided on the Contacts List. If not, the enquiry may be escalated to the 'on-call' Director to make the decision on disclosure.

For Critical enquiries, ONLY the following information will be disclosed:

- Whether they are known to named agencies
- Whether they are currently engaged with services.
- Known risk factors - to self or others.
- Diagnosis or nature of any potentially relevant health problem or condition, including mental health diagnosis.
- Recent significant life changes that can be established from patient records that may impact on behaviour.

2.6.3 A record of the personal information disclosed to partners by the MPS must be created. This should include what was shared and the reason for sharing. Any decision not to share information should similarly be recorded along with the reasons for the decision.

If sharing needs to occur in fast time and a Critical enquiry is made via telephone, a record must be similarly created on an MPS corporate system as soon as possible thereafter by the requestor.

2.7 Storage, Retention and Destruction of Information

Signatories to this agreement confirm that the appropriate storage and protection measures are in place for the information that is shared through this agreement.

2.7.1 If information is backed up and stored electronically via disc, hard drive, USB stick, or any mobile device, then adequate security measures must be in place on electronic systems. This specifically means that areas where shared information is stored can only be accessed via username and password. Permission to access the information shared by partners will be granted on a strict 'need to know' basis once it is contained within the electronic system, and an audit trail will capture events which evidence successful and unsuccessful access to the system and individual records. The media being used should then be stored in a physical location that has a level of security appropriate to the level that the information held is graded to.

2.7.2 If information shared under this agreement is printed it must be kept in a locked container within a secure premise with a managed access control. If printed information must be moved from its usual secure location, which is in accordance with the level of security required by this agreement, then any move temporary or permanent, must provide the same level of security in storage as per the original location. When documents are not being used they will be stored securely.

2.7.3 Access to the information in both electronic and paper formats will be limited to relevant staff on a need to know basis. The security and maintenance of security measures and passwords will be the responsibility of the Data Protection Officer/Caldicott Guardian or [Enter relevant role (e.g. ICT Security Officer)] within each agency. There will be a clear auditable access control system, detailing successful and unsuccessful attempts. The general public will have no access to either type of record.

2.7.4 All signatories will have appropriate policies and procedures governing the retention and destruction of records containing personal information retained within their systems.
As a general rule, signatories agree that personal information that has been shared will be destroyed immediately once it is no longer of relevance to the initial enquiry.

2.7.5 Electronic information will be disposed of by being weeded according to each agency's standard operating procedure in relation to their IT systems, being overwritten using an approved software utility or through the physical destruction of computer media.

2.7.6 Any paper records will be disposed of through a Restricted or Official Sensitive waste disposal system, using a shredder, or returned to the relevant Partner for secure disposal.

2.8 Confidentiality and Vetting

At a minimum, all the information to be shared under this agreement will be classified and managed in accordance with GSC.

Vetting is not mandatory to view this level of information; however the staff within the **London Borough of Bexley** Safeguarding Adults Service/relevant partner who will have access to police information are cleared to access this information within their own organisations. The information must only be processed (viewed) on a strict ‘need-to-know’ basis.

2.9 Transfer of Information - all agencies

Information will be transferred using secure email and preferably to and from a joint team mailbox to which appropriate staff have access, so that should the responsible individual be away, work can continue as normal. The mailbox will be checked regularly throughout the day.

Secure emails should be shared with the Bexley Safeguarding Adults Board Business Team as soon as possible and as emails change. It is the responsibility of the partner agencies to keep the BSAB informed.

2.9.1 It is recognised that email address ending ".gov.uk" and "nhs.uk" by themselves are **not secure** email addresses and so will not be used to share Official/ Sensitive level information.

2.9.2 In the event of a failure of the e-mail system, Partners reports and information forms will be shared via fax. A test sheet will be sent first to confirm the correct number has been inputted, and a response received, before the information is faxed across.

2.9.3 In cases of immediate risk, proactive and reactive sharing may occur using existing safeguarding referral processes following a telephone call to the department to make them aware of the report and to highlight any immediate action that has been completed / further actions required either by the relevant partner agency. Any sharing via telephone will be backed up in writing for audit purposes.

2.10 Security Incidents and Breaches of the Agreement

2.10.1 Security breaches must be reported to the relevant Caldicott Guardian or Data Protection Officer within 24 hours of occurring / being detected. A list of contacts can be found in Appendix G.

2.10.2 Partner agencies, if you wish to feature a reporting procedure for a breach please complete as prompted below and embolden the text once complete, please duplicate for multiple agencies.

The Concerned Partner Agency Contact must immediately inform the Bexley Safeguarding Adults Board Business Team of any security incident or breach of information, including unauthorised disclosure or loss of information, by calling the department or emailing bsab@bexley.gov.uk

2.10.2 The MPS SPOC must immediately inform the Information Assurance Unit of any security incident or breach of MPS information, including unauthorised disclosure or loss of information, by calling the department or emailing 'IAU Mailbox - Security Incidents'.

2.10.3 Partners confirm that security breaches are covered within their internal disciplinary procedures. If misuse is found, consideration will be given to facilitating an investigation into initiating criminal proceedings. All parties are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

2.11 Compliance

All partners are responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 1998/GDPR.

Partners agree where necessary to allow peer-to-peer reviews to ensure compliance with the security section of this agreement. Compliance with these security controls will be catered for in the periodic reviews of the agreement.

2.12 Review

This agreement will be reviewed six months after implementation and annually thereafter. In the event of a security incident or other issue which requires urgent attention, the parties may review the agreement more frequently.

2.13 Freedom of Information Act and Subject Access Requests

2.13.1 It is recognised that signatories to this agreement may receive a request for information made under the Freedom of Information Act 2000 that relates to the operation of this Agreement. Where applicable, they will observe the Code of Practice made under S.45 of the Freedom of Information Act 2000.

2.13.2 Normal practice will be to make all information sharing agreements available on relevant publication schemes.

2.13.3 The Freedom of Information Act Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. The Code also relates to the process by which one authority may transfer all or part of a request to another authority if it relates to information held only by the other authority.

2.13.4 Individuals can request a copy of all the information an organisation holds on them, by making a Subject Access Request (SAR). This may include information that was disclosed to that organisation under this agreement. Where this is the case, as a matter of good practice the organisation will liaise with the originating organisation to ensure that the release of the information to the individual will not prejudice any ongoing investigation/prosecution.

Section 3 - Legal Basis for information sharing and what can lawfully be shared

3.1 Data Protection Act 1998

It is the responsibility of all signatories to this Agreement to ensure that information exchanges are justified by, and in accordance with the Data Protection Act 1998.

The DPA 1998 acts as a framework for how to handle and process (including sharing, obtaining, recording and storing) personal and sensitive personal information. It contains two Schedules that list various Conditions which, when fulfilled, allow for the processing of personal data (Schedule 2) and sensitive personal data (Schedule 3). Personal data is that which can identify a living individual. Some personal data is classified as sensitive personal data when it relates to a person's racial or ethnic origins, physical or mental health or conditions, sexual life, criminal offences, religious beliefs and trade union membership. The 8 Data Protection Principles also need to be complied with to allow sharing to be lawful.

(Schedule 2, Schedule 3 and the 8 Data Protection Principles are listed in Appendix H)

3.1.1 Exemption from Fair and Lawful Processing (Principle 1)

Processing personal data for the purposes envisaged in Section 29 DPA - crime prevention or detection, or prosecution or apprehension of offenders is exempt from Principle 1, if complying with it would prejudice these purposes.

However, such processing must still satisfy one of the conditions in Schedule 2 DPA, and for sensitive personal data, one of the conditions in Schedule 3, DPA. Moreover, any disclosure must comply with the second through eight Data Protection Principles and any legal obligations owed outside of the DPA, such as confidentiality, as well as any professional responsibilities and obligations. If there is not valid consent, consideration should be given as to whether it is in the public interest to share the information.

3.1.2 Schedule 2, Data Protection Act 1998

To comply with Schedule 2, each case must be assessed on its own merit. Appropriate sharing of personal information through this agreement is likely to satisfy one of the following conditions in Schedule 2:

- **The data subject has consented to the processing [1]**
  This is applicable when an individual consents to their information being shared.

- **The processing is necessary in order to protect the vital interests of the data subject [4]**
  This is applicable when sharing a victim's information without consent for their own benefit, where if information was not shared, their life would be in immediate danger.

- **The data processing is necessary for the exercise of any functions conferred on any person by or under any enactment [5(b)]**
  This is applicable when sharing information for the purposes of a safeguarding enquiry under section 42 Care Act 2014, complying with a section 45 request for information from a SAB or when sharing through section 115 Crime and Disorder Act 1998 regarding offenders or suspected offenders.

- **The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of**

prejudice to the rights and freedoms of legitimate interests of the data subject[6(1)]

This is applicable where the sharing is necessary to fulfil common law duties and responsibilities of partner agencies, and where the sharing is done in such a way as to not disadvantage the rights of individual whose data is being shared.

3.1.3 Schedule 3, Data Protection Act 1998

In the vast majority of cases, the information potentially to be shared will be sensitive personal data and so will need to additionally satisfy one of the conditions in Schedule 3. Appropriate sharing of information will likely satisfy one of the following conditions:

- **The data subject has given his explicit consent to the processing of the personal data [1].**

- **The processing is necessary in order to protect the vital interests of the data subject where consent has been unreasonably withheld [3(b)]**

- **The processing is necessary for: the exercise of any function conferred on a person by or under an enactment [7(b)]**

- **The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph [10]**
  These circumstances are defined in Statutory Instrument 417/2000, which provides for sensitive personal information being processed where 'The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.' (Paragraph 10)

3.1.4 The 8 Data Protection Act Principles

All data that is to be shared is obtained for lawful purposes, connected with protecting and safeguarding vulnerable members of society and preventing criminal activities. Information will only be used and shared for the reason that the information was collected, and will be considered on a case by case basis. Only relevant information will be shared, which will be enough to fulfil the reason for disclosure but will not necessarily be all the information held by a partner agency about the Adult at Risk. The data will come from corporate information systems and will be subject to validation procedures so as to ensure data quality. Inaccuracies will be notified to originating agencies. Information will be historic in nature and therefore will not require updating. The length of time that information is required to be retained will vary depending on the case. However, once the information has been reviewed and it has been decided that it is no longer needed, it will be destroyed in accordance with the holding agency destruction policy. No information is to be transferred outside the UK. Therefore, compliance with this agreement should ensure compliance with the Data Act Principles.

In line with Principle 6 -

- Signatory agencies will respond to any notices from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.
- Signatories will comply with subject access requests in compliance with the relevant legislation.
- Signatories reserve the right to withdraw right of use of the data at any time.

3.2 Statutory Functions

3.2.1 Crime and Disorder Act 1998

A public authority must have some legal power entitling it to share the information. The Crime and Disorder Act 1998 recognises that key authorities, such as councils and the police, have a responsibility for the delivery of a wide range of services within the community. Section 17 places a duty on them to have due regard to the need to prevent crime and disorder in their area. Section 115 provides any person with the power, but not an obligation, to disclose information to relevant authorities (e.g. the police, health or local authorities) and their cooperating bodies where this is necessary or expedient for the purposes of any provision of the Act. Information sharing through this agreement is lawful under the Act as the objectives of this agreement contribute to these purposes.

3.2.2 Section 82 of the National Health Service Act 2006

This places a duty on the NHS and local authorities to cooperate with one another in order to secure and advance the health and welfare of people. NHS bodies will properly cooperate with and consider requests to share information, where appropriate and lawful to do so, will share that information.

3.2.3 Sections 13Z3 and 14Z23 NHS Act 2006 Restrictions

These sections place a general restriction on NHS England and Clinical Commissioning Groups in sharing information with others. However, disclosures for the purposes of safeguarding are permitted by these requirements.

3.2.4 The Care Act 2014

Sections 6 and 7 of the Care Act 2014 impose a general duty of co-operation between the local authority and other organisations providing care and support. This includes a duty on the local authority itself to ensure co-operation between its adult care and support, housing, public health and children's services.

Section 42 confers a legal power on the local authority to make enquiries in relation to Adults at Risk. As explained at section 1.3 above, this is an important area in which information sharing is provided for by this agreement.

Section 44 relates to the safeguarding adults review process and imposes an obligation on all members of the SAB to co-operate in and contribute to the carrying out of the review..

Section 45 of the Care Act 2014 imposes an obligation on organisations to comply with a request for information from a SAB for the purpose of enabling or assisting the SAB to perform its functions.

3.3 Human Rights Act 1998

3.3.1 Article 3: No torture, inhuman or degrading treatment

All statutory agencies have a pro-active responsibility to ensure that no person should be subjected to inhuman or degrading treatment. This includes Adults at Risk.

3.3.2 Article 8: The Right to Respect for Private and Family Life, Home and Correspondence

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Disclosing private information engages the right to respect for private life under article 8. However, effective sharing of information for the purposes set out in this agreement is to the direct benefit of the citizen and so in the public interest.

This agreement is in pursuit of a legitimate aim as it helps to protect Adults at Risk, contributes to the purposes of the Crime and Disorder Act 1998 and is in accordance with the Care Act 2014 and other similar legislation.

It is also proportionate as the amount and type of information shared will be compliant with the Data Protection Act 1998, and the minimum necessary to achieve the aims of this agreement, namely, to provide a better service and protection to Adults at Risk.

3.4 Consent (new consent rules under GDPR)

3.4.1 If consent is given by the data subject then it is clear to all concerned that there is no legal obstacle to sharing information. Where reasonably practicable and appropriate, informed consent should be sought. Whilst consent will provide a clear basis on which agencies can share personal data, this is not always achievable or desirable. For example, you should not ask for consent from the individual or their family in circumstances where you think this will be contrary to the Adult at Risk's welfare. For example, if the information is needed urgently then the delay in obtaining consent may not be justified. Seeking consent may prejudice a police investigation or may increase the risk of harm to the Adult at Risk.

3.4.2 Consent can be expressed orally or in writing, or can be inferred from the circumstances in which the information is given (implied consent). For example, a person who refers an allegation of abuse to a social worker would reasonably expect that information to be shared on a "need to know" basis with those responsible for investigating and following up the allegation. Implied consent is appropriate for the sharing of personal information however, express consent is required for the sharing of sensitive personal data. If there is valid consent, then it will last as long as the purposes for which that consent was given continue to exist, unless consent is withdrawn. Signatories should be aware that individuals have the right to withdraw consent at any time.

3.4.3 Practitioners should encourage clients to see information sharing (and giving their consent to share their personal information) in a positive light, as something which makes it easier for them to receive the services that they need. When seeking consent, signatories should be very clear about what they are asking for consent to do and to explain the potential ways and parties with whom information will be shared.

3.4.4 In order to ensure consent to the sharing of personal information is informed, any professional must give victims standard documentation about 'Sharing Information' at the first point of contact. It is clearly an issue of great importance as to whether an individual has provided valid

3.4.5. Professionals should avoid giving absolute guarantees as to confidentiality, particularly when dealing with disclosures from children. In such cases it should be made clear from the outset that what is said will be treated in confidence but such information may need to be passed on to other professionals who may need to know.

3.4.6 Where the data subject does not have capacity to give consent to share information, consent may be sought from someone who may appropriately act on their behalf, for example, If the adult has previously granted an applicable power of attorney, the donee of the power of attorney can consent on their behalf.

3.5 How Adults at Risk will be Assessed for their Mental Capacity to Give Consent

3.5.1 All adults are presumed to have the capacity to give or withhold their consent to the sharing of confidential information, unless there is evidence to the contrary. It is likely that a percentage of adults at risks subject to this information sharing agreement will lack the mental capacity to make particular decisions for themselves because of existing health issues or infirmity. The Mental Capacity Act 2005 provides the legal framework for acting and making decisions on behalf of individuals who lack the mental capacity. The A*ct* defines a person who lacks capacity as a person who lacks capacity to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken.

3.5.2 Section 1 of the Act sets out the five statutory principles that apply to mental capacity:

1. A person must be assumed to have capacity unless it is established that they lack capacity
2. A person is not to be treated as unable to make a decision unless all practicable steps to help him to do so are taken without success
3. A person is not to be treated as unable to make decisions merely because he makes an unwise decision
4. An act done or decision made, under this Act for or on behalf of a person who lacks capacity must be done, or made, in their best interests[2]
5. Before the act is done, or the decision made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is least restrictive of the person's rights and freedom of action

3.5.3 Signatories will deal with capacity issues in accordance with these principles. Where there is doubt or difficulties arise in relation to capacity, advice should be sought from appropriately qualified mental health professionals.

3.6 Public Interest

3.6.1 If consent to sharing of information has **not** been given, a professional must consider whether there is a pressing need to disclose the information. The rule of proportionality should be applied to ensure a fair balance is achieved between the public interest and the rights of the individual affected. The same overall test is applied whether the data subject is the Adult at Risk, the suspected perpetrator of abuse or a third party.

3.6.2 Signatories understand that when considering whether disclosing the information would be in the public interest, the following criteria will be of particular relevance:

- Is there credible evidence giving reasonable cause to believe that an adult is suffering, or is at risk of suffering, serious harm?
- Is the disclosure needed to protect the vulnerable adult's vital interests?
- Is the disclosure needed to detect or prevent crime?
- Does the body seeking the information have a legitimate interest in receiving it?
- Is the extent of the information disclosed and the number of people to whom it is disclosed no greater than is required to achieve the relevant aims?
- How great is the risk if disclosure is not made?

3.6.3 When considering whether disclosure is in the public interest, the rights and interests of the individual affected by disclosure must be taken into account. Signatories should consider:

- Is the intended disclosure relevant and proportionate to the intended aim?
- What is the impact of disclosure likely to be on the individual?
- Is there another equally effective means of achieving the same aim?

[2] A 'Best Interests' checklist can be found in Section 4 Mental Capacity Act 2005

3.6.4 The more sensitive the information, the greater the need to justify disclosure and the greater the need to ensure that only those professionals who have to be informed receive the information.

3.6.5 NHS bodies will also have to consider the Department of Health Code of Practice on Confidentiality, as well as the General Medical Council Guidance, in respect of patient data they hold.

3.6.6 If information is disclosed without consent, it is essential that there is a clear record of the reasons and justification for disclosure so as to demonstrate that the decision is reasonable, proportionate and justifiable.

3.6.7 The Care Act 2014 statutory guidance advises that the first priority should always be to ensure the safety and well-being of the adult.

3.7 Common Law - Duty of Confidence

3.7.1 Personal information held by public authorities is subject to a common law duty of confidence, and is owed to the person who has provided information on the understanding it is to be kept confidential and, in cases of medical or other private records, the person to whom the information relates.

3.7.2 The Courts have found a duty of confidentiality to exist in a number of circumstances –

- where the information is confidential in nature, is more than trivial, and is not publically known. It has been imparted in circumstances importing an obligation of confidence and it's disclosure (or use outside the expected parameters of use) would cause detriment to any person
- a contract provides for information to be kept confidential
- there is a special relationship between parties, such as patient and doctor, solicitor and client, teacher and pupil, which implies confidentiality obligations
- an agency or a Government department, such as Inland Revenue, collects and holds personal information for the specific purposes of its functions.

3.7.3 However, an obligation of confidence, including where there is a confidential relationship, is not absolute and can be overridden without breaching common law duty if:

- the information is not confidential in nature;
- the person to whom the duty is owed has given consent;
- there is an overriding public interest in disclosure (see above, **Public Interest**); or
- disclosure is required or permitted by a court order, legislation or other legal obligation.

3.6.4 Some information may not be confidential, particularly if it is trivial or readily available from other sources or if the person to whom it relates would not have an interest in keeping it secret. For example, a Social Worker who was concerned about the whereabouts of their client, might telephone a family member or employer to establish where the adult was that day.

3.8 Maintaining Confidentiality

As a general rule you should treat all personal information you acquire or hold in the course of working with adults at risk as confidential and take particular care that sensitive information is held securely. Anyone who receives information, knowing it is confidential, is also subject to the duty of confidence. Whenever you give or receive information in confidence you should ensure that there is a clear understanding as to how it may be used if

shared. Where information is shared under this agreement, the terms of this agreement provide for this.

3.9 Medical Emergency

In emergency medical situations information should always be shared between partner agencies, otherwise not sharing could place a vulnerable member of the public at increased risk of significant harm. In circumstances where vulnerable members of the public carry emergency alert cards, the instructions on the card should be followed in line with service procedures.

If consent has not been sought, or sought and withheld, the agency must consider if there is a legitimate purpose for sharing the information and if it is in the public interest to share; and clearly record the reasons for doing so.

3.10 Fair Processing

Practitioners will be open and honest with vulnerable adults, carers, and others about why, what, how and with whom information will or could be shared with other agencies.

3.10.1 When data is obtained from data subjects, they must, so far as practicable, be provided with, or have made readily available to them, the following information so as to ensure processing is fair to the data subject:

a) The identity of the data controller
b) If the data controller has nominated a representative for the purposes of the Act, the identity of that representative
c) The purpose or purposes for which the data are intended to be processed
d) Any further information which is necessary, taking into account the specific circumstances in which the data is or will be processed

3.10.2 Where information about a data subject has been obtained from a third party, organisations must ensure that the data subject has ready access to the fair processing information, so far as practicable, either before the data is first processed or as soon as practicable after that time. Where possible, steps should be taken to provide data subjects with the information listed above.

3.10.3 In order to comply with the above obligations, and as required by the Information Commissioners Office Registration, signatories will have a Fair Processing Notice in place and readily accessible for inspection by the public.

3.11 Summary

There are no legal barriers that prevent the appropriate and necessary sharing of information between agencies in fulfilment of their statutory duties to safeguard vulnerable adults, provided that proper agreed procedures are followed.

A flowchart can be found in Appendix J that summarises when information can and **can not** be shared.

Section 4 - Agreement to abide by this arrangement

The signatories to this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the terms of this agreement.
- Ensure that the procedures set out in this agreement are complied with.
- Ensure that all information will be shared where this is lawful and permitted by this agreement.
- Engage in a review of this agreement with the other signatories six months after its implementation and annually thereafter.

We the undersigned agree on behalf of each agency/organisation to the terms of this information sharing agreement:

Agency	Post Held	Name	Signature	Date
MPS South East BCU	**SE BCU Tri-Borough Commander**	**Simon Dobinson**		
London Borough of Bexley	**Chief Executive**	**Gill Steward**		
Bexley Safeguarding Adults Board	**BSAB Independent Chair**	**Annie Callanan**		
Bexley Clinical Commissioning Group, SE CCG	**Single Accountable Officer**	**Andrew Bland**		
Oxleas NHS Foundation Trust	**Chief Executive**	**Helen Smith**		
Lewisham & Greenwich NHS Trust	**Chief Executive**	**Ben Travis**		

Dartford Gravesham NHS Trust	**Chief Executive**	**Gerard Sammon**		

Appendix A – Six Key Principles of Adult Safeguarding

1. Empowerment
People being supported and encouraged to make their own decisions and informed consent.

"I am asked what I want as the outcomes from the safeguarding process and these directly inform what happens."

2. Prevention
It is better to take action before harm occurs.

"I receive clear and simple information about what abuse is, how to recognise the signs and what I can do to seek help."

3. Proportionality
The least intrusive response appropriate to the risk presented.

"I am sure that the professionals will work in my interest, as I see them and they will only get involved as much as needed."

4. Protection
Support and representation for those in greatest need.

"I get help and support to report abuse and neglect. I get help so that I am able to take part in the safeguarding process to the extent to which I want."

5. Partnership
Local solutions through services working with their communities. Communities have a part to play in preventing, detecting and reporting neglect and abuse.

"I know that staff treat any personal and sensitive information in confidence, only sharing what is helpful and necessary. I am confident that professionals will work together and with me to get the best result for me."

6. Accountability
Accountability and transparency in delivering safeguarding.

"I understand the role of everyone involved in my life and so do they."

Appendix B - Abuse and Criminal offences that Adults at Risk may become victims of.

Below are the main forms of abused defined.

- **physical abuse**, including hitting, slapping, pushing, kicking, misuse of medication, restraint, or inappropriate sanctions
- **sexual abuse**, including rape and sexual assault or sexual acts to which the adult at risk has not consented, or could not consent or was pressured into consenting

- **psychological abuse**, including emotional abuse, threats of harm or abandonment, deprivation of contact, humiliation, blaming, controlling, intimidation, coercion, harassment, verbal abuse, isolation or withdrawal from services or supportive networks.
- **financial or material abuse**, including theft, fraud, exploitation, pressure in connection with wills, property or inheritance or financial transactions, or the misuse or misappropriation of property, possessions or benefits
- **neglect and acts of omission**, including ignoring medical or physical care needs, failure to provide access to appropriate health, social care or educational services, the withholding of the necessities of life, such as medication, adequate nutrition and heating
- **Discriminatory abuse**, including racist, sexist, that based on a person's disability, and other forms of harassment, slurs or similar treatment.

A number of the other most significant laws relating to abuse faced by Adults at Risk are:

- **The Domestic Violence, Crime and Victims Act 2004** explicitly states that it is a criminal offence to physically or sexually abuse, harm or cause deliberate cruelty by neglect of a child or an adult. This legislation was introduced, in part, to emphasise the crime of abuse between partners within the home.
- **Mental Capacity Act 2005.** Creates an offence of ill-treatment or wilful neglect of a person lacking capacity by anyone responsible for that person's care.
- **Offences Against The Persons Act 1861** including grievous bodily harm with intent, grievous bodily harm, chokes /suffocates/strangles, unlawfully applies drugs with intent to commit indictable offence, poisoning with intent to endanger life/cause GBH or with intent to injure, aggrieve or annoy and assault occasioning actual bodily harm.
- **Criminal Justice Act 1988** including Common assault,
- **Medicines Act 1968** including: Unlawfully administering medication, Injuriously affecting the composition of medicinal products
- **The Sexual Offences Act 2003**
- **Public Order Act 1986** including affray, fear or provocation of violence, intentional harassment, alarm or distress, and harassment/alarm or distress
- **Protection from Harassment Act 1977** including course of conduct amounting to harassment, injunctions against harassment, and course of conduct that causes another to fear.
- **Theft Act 1968** including dishonest appropriation of property, robbery, burglary dwelling house, blackmail
- **Mental Health Act 1983** including ill treatment or neglect of mentally disordered patients within hospital or nursing homes or otherwise in persons custody or care and unlawful sexual intercourse with patients/residents suffering mental disorder.
- **Criminal Justice and Courts Act 2015 sec 20-25 -** offences involving ill treatment or wilful neglect
- **Modern Slavery Act 2015 Section 52 –** duty to notify Secretary of State about suspected victims of slavery or Human Trafficking

Appendix C - The National Standards - Headline Standards [3]

Standard 1	Each local authority has established a multi-agency partnership to lead 'Safeguarding Adults' work
Standard 2	Accountability for and ownership of 'Safeguarding Adults' work is recognised by each partner organisation's executive body.
Standard 3	The 'Safeguarding Adults' policy includes a clear statement of every person's right to live a life free from abuse and neglect, and this message is actively promoted to the public by the Local Strategic Partnership, the 'Safeguarding Adults' partnership, and its member organisations.
Standard 4	Each partner agency has a clear, well-publicised policy of Zero-Tolerance of abuse within the organisation.
Standard 5	The 'Safeguarding Adults' partnership oversees a multi-agency workforce development/training sub-group. The partnership has a workforce development/training strategy and ensures that it is appropriately resourced.
Standard 6	All citizens can access information about how to gain safety from abuse and violence, including information about the local 'Safeguarding Adults' procedures.
Standard 7	There is a local multi-agency 'Safeguarding Adults' policy and procedure describing the framework for responding to all adults "who are or may be eligible for community care services" and who may be at risk of abuse or neglect.
Standard 8	Each partner agency has a set of internal guidelines, consistent with the local multi-agency 'Safeguarding Adults' policy and procedures, which set out the responsibilities of all workers to operate within it.
Standard 9	The multi-agency 'Safeguarding Adults' procedures detail the following stages: Alert, Referral, Decision, Safeguarding assessment strategy, Safeguarding assessment, Safeguarding plan, Review, Recording and Monitoring.
Standard 10	The safeguarding procedures are accessible to all adults covered by the policy.
Standard 11	The partnership explicitly includes service users as key partners in all aspects of the work. This includes building service-user participation into it's: membership; monitoring, development and implementation of its work; training strategy; and planning and implementation of their individual safeguarding assessment and plans.

[3] Safeguarding Adults ADSS, 2005

Appendix D –
Caldicott Principles (September 2013) – Health and Social Care

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

Principle 2
Don't use personal confidential data unless it is absolutely necessary
Personal confidential data should not be included unless it is essential for the specified purposes of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s)

Principle 3
Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out

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

Principle 5
Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality

Principle 6
Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements

Principle 7
The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

Appendix E - Form 87V & 87VA

METROPOLITAN POLICE

TOTAL POLICING

Form 87V

INFORMATION REQUEST

Subject's Name:		Date of Birth:		Police URN:	

Originator			
Name/Position:			
Address:		Post Code:	
Tel. No.:		Email address:	

Number of Subjects Requiring Checks		(USE ONE FORM PER SUBJECT)					
Name:		Location:					
Date of Birth:		Male	☐	Female	☐	Ethnicity	☐
Address:							

Reason for Information Request (London Multiagency safeguarding Adult Guidance)		Y	N
(A)	Inter-Agency Risk Management (MAPPA).	☐	☐
(B)	Initial Assessment to justify Safeguarding investigation	☐	☐
(C)	To assess the risk to the adult at risk and others	☐	☐
(D)	To put in place protective measures	☐	☐
Consent must be sought for B, C and D from subject. If YES, where recorded? Unless overridden by Authorising person under Public interest (recorded)		☐	☐

Supporting Circumstances / allegation (MUST BE COMPLETED)

Read & Signed by Person Requesting - Manager

TO BE DEVELOPED BY LONDON PARTNERSHIP XXXXXXXXXXXXXXXXXXXXXXXXXX

Signed:		Print Name:		Date:	

Police Use only

Signed authority to carry out checks (DS or above)

Signed:		Print Name:		Date:	

Retention Period: 7 Years
MP 65/14

METROPOLITAN POLICE

TOTAL POLICING

Information Request- RESULT

This information is sent in confidence and is restricted. It must not be passed on to a third party without the express permission of the police.

For: (Name of recipient)
Of: (Name and address of department, section, team or unit)

The following is a summary of information obtained from police checks relating to the subjects specified below. The summary has been de-personalised in accordance with the Data Protection Act 1998 and consists only of sufficient information which is assessed as being necessary and relevant for the purposes specified on the original request.

Name of Subject	Summary of information known

No further action	**Yes** ☐ **No** ☐	**Form 87 URN**	
If 'Y' state what action			

Supervisor (Sergeant) authorising disclosure Signature					
Signed:		**Print Name:**		**Date:**	

Retention Period: 7 Years
MP 67/14

Appendix F - Confidentiality Statement

Meeting confidentiality statement / ISP Summary Brief

Chair		Date of Meeting	

Information discussed by the agency representatives, within the ambit of this meeting, is strictly confidential and must not be disclosed to third parties.
All agencies should ensure that all minutes and related documentation are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

THE PURPOSE OF THE MEETING IS AS FOLLOWS:

- To share information to increase the safety, health and well- being of victims – adults and/or their children; and/or
- To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm; and/or
- To reduce repeat victimisation; and/or
- To improve agency accountability; and/or
- Improve support for staff involved in high risk cases.

BY SIGNING THIS DOCUMENT WE AGREE TO ABIDE TO THESE PRINCIPLES.

Meeting Confidentiality agreed / ISP Agreed (attendees)

Agency	Name of Representative	Signature	Email

Appendix G
Partners Contacts List for Critical Enquiries, Escalations and Incidents of Security Breaches

(to be completed locally – examples below)

Data Protection Officer
Nick Hollier
Data Protection Officer
Deputy Director Corporate Services
0203 045 4091
data.protection@bexley.gov.uk

Caldicott Guardian
Stuart Rowbotham
Caldicott Guardian
Director of Adult Social Care and Health
0203 045 5863
caldicott.guardian@bexley.gov.uk

Critical Enquiries

Escalations

Appendix H- Data Protection Act 1998 8 Principles, Schedules 2 & 3

Principle 1	The first data protection principle states that data must be processed lawfully and fairly.
Principle 2	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Principle 3	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Principle 4	Personal data shall be accurate and, where necessary, kept up to date.
Principle 5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
Principle 6	Personal data shall be processed in accordance with the rights of data subjects under this Act.
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Principle 8	Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

SCHEDULE 2 - Conditions relevant for purposes of the first principle: processing of any personal data[4]

1. The data subject has given his consent to the processing
2. The processing is necessary -

   (a) for the performance of a contract to which the data subject is a party, or

   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject
5. The processing is necessary -

   (a) for the administration of justice,

   (aa) for the exercise of any functions of either House of Parliament,

   (b) for the exercise of any functions conferred on any person by or under any enactment,

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

[4] Correct as of November 2016

SCHEDULE 3 - Conditions relevant for purposes of the first principle: processing of sensitive personal data[5]

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order -

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary -

(a) in order to protect the vital interests of the data subject or another person, in a case where -

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing -

(a) is carried out in the course of its legitimate activities by any body or association which-

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing -

[5] Correct as of November 2016

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary -

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order -

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A (1) The processing -

(a) is either -

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph “an anti-fraud organisation” means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8. (1) The processing is necessary for medical purposes and is undertaken by -

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing -

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

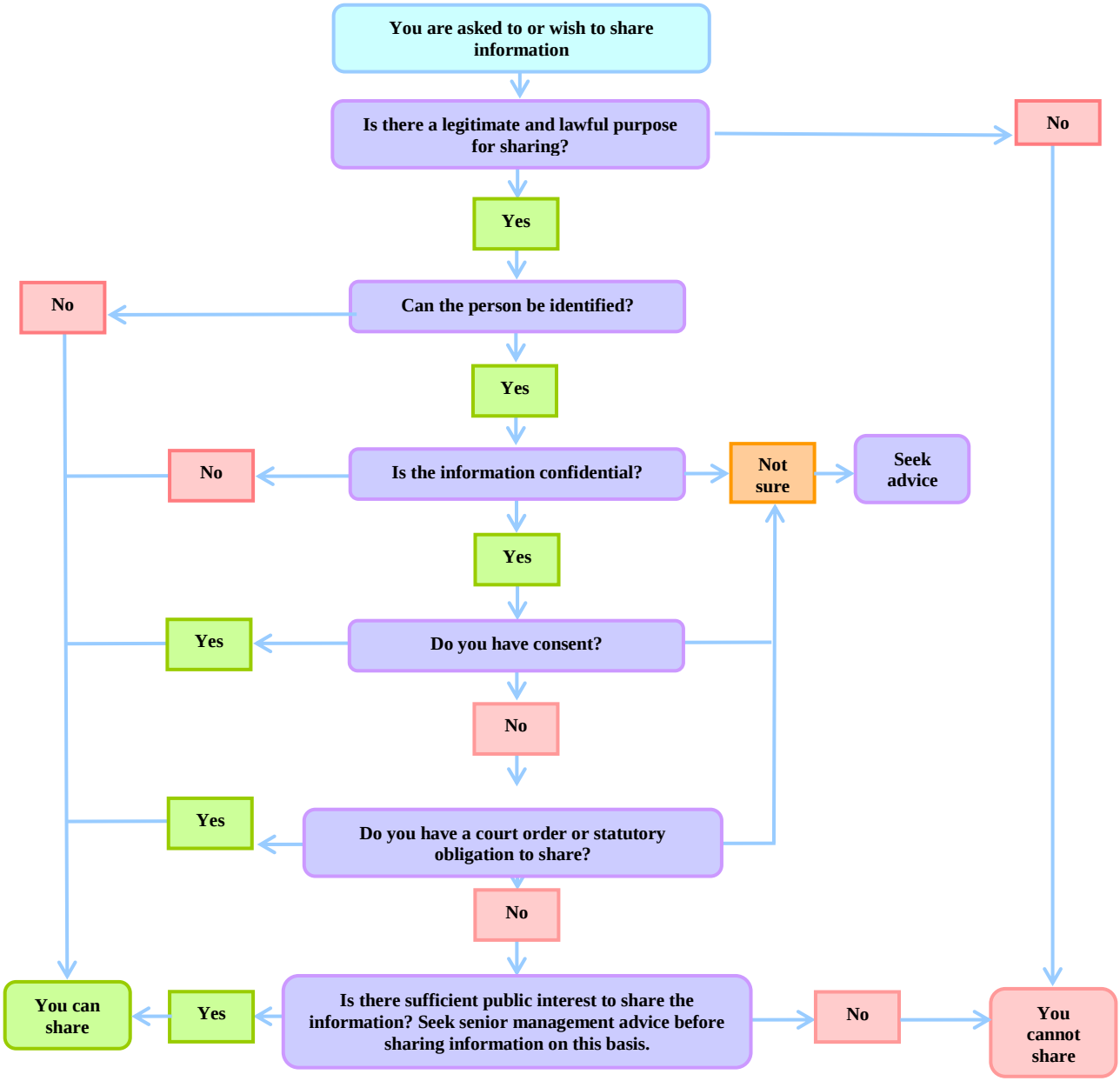
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix I – Information sharing flowchart



Share information:

- Identify how much information to share and the relevance
- Ensure you are getting the right information to the right person
- Ensure you are sharing the information securely
- Inform the person that the information has been shared if they were not aware of this and it would not create or increase risk of harm

Record information is going to be shared and your reasons in line with your agency's procedures

If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

(Source: HM Government: Information Sharing Pocket Guide)