This Data Sharing Agreement should be used if you are processing personal data for the law enforcement purposes[1], as described under Part 3 of the Data Protection Act (DPA) 2018.

Data Sharing Agreement

Between

Lambeth Safeguarding Adults Board

London Borough of Lambeth,

Metropolitan Police Service

Kings College Hospital NHS Foundation Trust, Guys and St Thomas' Hospital NHS Foundation Trust, South London and Maudsley NHS Foundation Trust,

Lambeth Council Adult Social Care Service

Lambeth Clinical Commissioning Group

and

Other relevant partners (see enclosed)

for the purpose of Safeguarding Adults at Risk within the London Borough of Lambeth

[1] *"the law enforcement purposes" are the purposes of the 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.*

Freedom of Information Act Publication Scheme	
Government Security Classification	Official
Publication Scheme Y/N	Yes
Title	A purpose specific data sharing agreement between Lambeth Safeguarding Adults Board London Borough of Lambeth Metropolitan Police Service Central South NHS Lambeth Clinical Commissioning Group Guy's and St Thomas' NHS Foundation Trust Kings College Hospital NHS Foundation Trust South London and Maudsley Mental Health NHS Foundation Trust And all other listed partners
Version	1.1
Summary	An agreement to formalise information sharing arrangements for the Adults at Risk partnership
BCU or Unit, Directorate	Central south
Author	London Safeguarding Adults Board
Review Date	April 2022
Date Issued	April 2019
ISA Ref:	N/A

Table of Contents

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 Safeguarding Adults Board (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.

The statutory guidance under the Act states that six key principles underpin all adult safeguarding work. These apply across all agencies involved in the process. These principles can be found in Appendix A.

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 Signatory Organisations 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.

Section 1 - The Purpose of the Agreement

1.1 This Agreement –

- describes 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 they will deal with those requests;

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

- describes the roles and structures that will support the exchange of information between the signatory organisations, and security procedures necessary to ensure compliance with responsibilities under the Data Protection Act, Caldicott Principles and organisation 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: in particular it will not be a breach of the agreement for a signatory organisation to refuse to share information where disclosure of such would constitute a breach of legal or professional obligations owed by that Signatory Organisation in respect of that information.

1.2 Scope of this Data Sharing Agreement

The signatories to this agreement are all Members of the Lambeth Safeguarding Adults Board.

This agreement **does** cover the sharing and assessing of information held by the Signatory Organisations by:

- **Central South Borough Command Unit** 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 social care needs

This agreement **does not** cover the sharing and processing of information held by the Signatory Organisations for the purposes of:

- Public Protection Unit (Jigsaw) through MAPPA process
- **Central South** Prolific Priority Offender Unit
- **Central South DV** Multi Agency Risk Assessment Conference (MARAC) information sharing
- **Central South** Community MARAC
- Disability Targeted Hate Crime - managed under the current MPS Hate Crime Policy
- Domestic Abuse - managed under the current Domestic Abuse Policy
- Information required by the police for criminal investigations

These activities are covered by separate legislation and 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 or 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 Organisation 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 the professional/Signatory Organisation believes or suspects that a crime has been committed or that the individual is immediately at risk.

Explanations of the type of abuse and criminal offences of which Adults at Risk may become victims, 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 Care Quality Commission (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 (ADASS) 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 is noted that Standard 9 language is not Care Act compliant, however the equivalent enquiry process and stages applies. 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 among the Signatory Organisations and drawing upon partner organisations' specialist skill sets, all Signatory Organisations can offer the best possible service to safeguard adults at risk 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 suspected abuse or neglect have an important part to play, especially if the adult at risk lacks capacity. In such cases, the friends or family should be consulted, where practicable, in line with the Mental Capacity Act 2005. The role of Signatory Organisation 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 and be aware of issues regarding abuse, neglect or exploitation. The document recognises variation in terminology between Signatory Organisations 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 Signatory 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 disclosure of any particular information should be proportionate and necessary for the purposes of safeguarding.

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 ("Personal Data" and "Special Category data and Conviction Data" in the language of the Data Protection Act 2018) needs to be shared to allow relevant Signatory Organisations to identify these individuals and explain why they are a risk to vulnerable adults

(the "Adult at Risk"). Examples of the kind of personal & special category and conviction data that may be shared include:

- Personal identifiers (names, addresses, dates of birth)
- Current photograph of the suspected offender (if appropriate)
- Descriptive information (photographs, marks, scars)
- 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 organisational action;
- The nature and circumstances of the ongoing risk to the Adult at Risk.

1.4.3 Personal information Disclosed about Third Parties may include:

- Adult at Risk relevant family members or other personal contacts
- 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 at Risk. Information shared on these individuals must be necessary to assist in the assessment of safeguarding needs and delivery of safeguarding services and only the minimum required for these purposes.

Information considered for sharing in regard 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 Signatory Organisations that is **relevant** to assisting partners in services or duties towards the adult at risk concerned.

This information may need to be shared to enable Signatory Organisations 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 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 of Official Sensitive.

2.2 Accuracy of Information

If information held is found to be inaccurate, the Signatory Organisation producing the information will be notified. The producing Signatory Organisation 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.

2.3 How the Information will be processed

2.3.1 The sharing of information between Signatory Organisations may be proactive or as a result of a request for information. Signatory Organisations will inform the police about Adults at Risk where a crime may have been committed and equally, police will notify Safeguarding Adults Services and the relevant NHS bodies 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 recipient Signatory Organisations.

Information handling and requests by the Metropolitan Police Service (MPS)

2.3.2 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 **Central South** police Public Protection Desk (PPD) / Multi Agency Safeguarding Hub (MASH) contact. If deemed appropriate and necessary to do so to protect and safeguard the adult at risk, they will share the ACN on to **Lambeth's** relevant partnership team via the secure email link within MERLIN.

Information handling and requests by the Local Authority

2.3.3 Any requests under a Section 42 Care Act enquiry must be dealt with expeditiously. Any requests from the Local Authority to partner Signatory Organisations must be in a written format and for police information. Requests to any partner Signatory Organisation asking for information will include reasons why they require any relevant information held. In the case of requests to police, the completed form will be sent to the Borough PPD/MASH or BCU Mental Health Team. For criminal investigations, partner Signatory Organisations should initially liaise with the police officer in charge of the enquiry.

2.3.4 The PPD or designated BCU 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 adequate, relevant and not excessive for disclosure, for the specified, explicit and lawful purpose requested.

2.3.5 Any Signatory Organisation refusal to share information under Section 42 Care Act 2014 must be in writing and 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.

2.3.6 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 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.

Information sharing by NHS bodies

2.3.7 Where information is held or sought by a NHS body, the following process will be used for sharing information:
All requests for information should go to the respective clinical team who will consider the information gathered and decide (with reference to organisational policies) whether it is adequate, relevant and proportionate for disclosure for the specified purpose requested. If there are any doubts about the legitimacy of sharing information for safeguarding purposes, the clinical team will discuss with their trust adult safeguarding lead, Caldicott Guardian, & Senior Information Risk Owner, prior to releasing the information.

Information sharing by London Ambulance Service

2.3.8 London Ambulance Service (LAS) will share information about safeguarding concerns and staff identify with the local authority and police as appropriate and in line with multi agency policy and procedures. London Ambulance Service will share its involvement and attendance at patients identified by Safeguarding Adults Board (SAB) & Safeguarding children's Board (SCB) to support investigations including Serious Adult Reviews (SARs) and Serious Children's Reviews (SCRs). Information shared pursuant to this agreement will be disclosed in accordance with the LAS flowcharts for raising a safeguarding concern and/or welfare concerns.

Information sharing at safeguarding meetings and case conferences

2.3.9 Should a meeting be called to discuss a case, a Confidentiality Statement will be read out by the Chair/Safeguarding Adults Manager to all attending parties, which outlines that information shared at the meeting is strictly confidential and must not be discussed with or disclosed to third parties.
A sample Confidentiality Statement and Register can be found in Appendix F.

Onward disclosure of shared information

2.3.10 Permission must be sought by the Signatory Organisations from the relevant partner organisation 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 the purposes of safeguarding an Adult at Risk. This may include policing purposes, and/or the provision of care and support. All requests made should be done so by either secure e-mail or in writing so that an audit trail exists.

2.4 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 Adults at Risk, 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.

2.4.1 Initial contact for Critical enquiries will be made using the usual methods of obtaining information from relevant parties. However, in addition the relevant Board Member will be notified. In the event that the relevant person cannot be contacted a locally agreed escalation policy should be followed.

2.4.2 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 [*insert relevant partner agency*].
- 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.

2.4.3 A record of the personal information disclosed to other Signatory Organisations 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 appropriate MPS corporate system as soon as possible thereafter by the requestor.

2.5 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.

2.5.1 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, and appropriate encryption measures are in place. Permission to access the information shared by Signatory Organisations 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.

Where removable media is used, MPS personnel must only use an encrypted MPS approved Datashur USB. CDs are no longer acceptable.

2.5.2 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.

2.5.3 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 within each Signatory Organisation. 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.

2.5.4 All Signatory Organisations will have appropriate policies and procedures governing the retention and destruction of records containing personal information retained within their systems. These policies and procedures must be followed. Once the minimum retention period has expired, a risk assessment should be undertaken of whether the records should be kept for longer, if necessary. If not the records should be promptly and securely destroyed.

2.5.5 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.

2.5.6 Any paper records will be disposed of through an OFFICIAL SENSITVE waste disposal system, using a cross shredder, or returned to the relevant Signatory Organisation for secure disposal.

2.6 Confidentiality and Vetting

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

Vetting is not mandatory to view this level of information; however, the staff within **Lambeth** 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.
Use the link below to access the Government Security Classifications[2]

2.7 Transfer of Information - all agencies

Information will be transferred using approved secure email (such as Egress) and preferably to and from a joint team mailbox to which appropriate staff have access, so should the responsible individual be away, work can continue as normal.

2.7.1 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 information

[2]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

without use of a further appropriate encryption method[3]. Please see appendix H for a guide to sharing sensitive information by email, for Health and Social Care Email Users.

2.7.2 In the event of a failure of the e-mail system, reports will need to be done via telephone.

2.7.3 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.

2.8 Security Incidents and Breaches of the Agreement

2.8.1 Security breaches, including misuse of MPS information, must be reported to the relevant Single Point of Contact (SPOC), Caldicott Guardian or Data Protection Officer (DPO) without undue delay of occurring/or no later than 24 hours after becoming aware of it. This is to allow the MPS to risk assess the security incident or breach of the Agreement, in circumstances where the security breach concerns MPS INFORMATION. A list of contacts can be found in Appendix G.

It is still the responsibility of All Signatory Organisations to comply with the obligations laid out under Section 67 and 68 of the DPA 2018.

2.8.2 Where a security incident involves health or social care information, the NHS Digital *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation* will be followed.

2.8.3 The MPS SPOC must immediately inform the Information Assurance Unit (IAU) 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'.

All other partners should have a reporting procedure for a breach. Process should revert to internally agreed policy and procedure.

2.8.4 Signatory Organisations 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 Signatory Organisations are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

2.9 Compliance

All Signatory Organisations are responsible for ensuring the security controls are implemented and staff are aware of (and where appropriate, trained in) their responsibilities under the Data Protection Act 2018.

Signatory Organisations 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.

[3] Secure email options are CJSM, pnn, nhs.net, gsi and Egress.

2.10 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 Signatory Organisations may review the agreement more frequently.

2.11 Freedom of Information Act and Subject Access Requests / Right of Access Requests

2.11.1 It is recognised that Signatory Organisations 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 in responding to the request.

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

2.11.3 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.

2.11.4 Individuals can request a copy of all the information an organisation holds on them, by making a Subject Access Request (SAR). The MPS refer to these requests as Right of Access Requests (ROAR) under the DPA 2018. This may include information that was disclosed to a Signatory Organisation under this agreement. Where this is the case, as a matter of good practice the Signatory Organisation in receipt of the SAR/ROAR will liaise with the originating Signatory Organisation to the information to ensure that the release of the information to the individual will not prejudice any ongoing investigation/prosecution, or engage other exemptions within the Data Protection Act 2018.

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

3.1 General Principles

All information exchanges between the Signatory Organisations must be:

- In accordance with the law (see section 3.2 below);
- 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 (described in section 3.11 below).

3.2 Data Protection Act 2018 (the "DPA")

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

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

The DPA acts as a framework for how to handle and process (including sharing, obtaining, recording and storing) personal and special category personal information. It contains two Schedules that list various Conditions which, when fulfilled, allow for the processing of personal data (Schedule 1) and special category data (Schedule 8). Personal data is that which can identify a living individual. Some personal data is classified as special category 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 6 Data Protection Principles also need to be complied with to allow sharing to be lawful.

(The 6 Data Protection Principles are listed in Appendix H)

3.2.1 Lawful and Fair Processing (Principle 1)

Signatory Organisations are exempt from complying with their 'obligations' and the 'rights of the individual' as described in the DPA, if it would be likely to prejudice the prevention or the detection of crime, the apprehension or prosecution of offenders.[4]

Fair Processing Notices inform individuals of what we do with their personal data, however even though the processing is lawful and fair, it is the level of transparency to which we are exempt, if it would prejudice any of the law enforcement purposes. Therefore Principle 1 cannot always be fully complied with.

Any disclosure must still comply with the Data Protection Principles and legal obligations owed outside of the DPA 2018, 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.

[4] Schedule 2, Part 1, Section 1(b) Section 2(1)(a)(b) and Section 2(2) and 2(3) DPA 2018

3.2.2 Schedule 1 (Part 2 and Part 3) Data Protection Act 2018

To comply with Schedule 1, 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 1:

- **This condition is met if the data subject has given consent to the processing [29]**
  This is applicable when an individual consents to their information being shared.
  [Schedule 1, Part 3 condition 29 DPA]

Or alternatively,

- **The processing is necessary to protect the vital interests of an individual, and: the data subject is physically or legally incapable of giving consent [30]**
  This is applicable when sharing a victim's information without consent, for their own benefit and where if information was not shared, their life would be in immediate danger.
  [Schedule 1, Part 3 condition 30 DPA]

- **The data processing is necessary for the purpose of the exercise of a function conferred on a person by an enactment or rule of law [6(1)]**
  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.
  [Schedule 1, Part 2 condition 6(1) DPA]

- **The processing is necessary for the exercise of any functions of a public nature exercised in the public interest by any person [36]**.
  Even where the sharing of information is not designed to meet a precise statutory function, if the processing is being done to discharge public function and the public interest favours disclosure, the Data Protection Act permits it.
  [Schedule 1, Part 3 sec 36 DPA]

- **The processing is necessary for the purpose of legitimate interests pursued by the 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 [10(1)(2)(3)]**
  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.
  [Schedule 1, Part 2 section 10(1)(2)(3) DPA]

3.2.3 Schedule 8 of the Data Protection Act 2018

In the vast majority of cases, the information potentially to be shared will be special category personal data and so will need to additionally satisfy one of the conditions in Schedule 8. Appropriate sharing of information will likely satisfy one of the following conditions:

- **The processing is necessary to protect the vital interests of the data subject or of another individual [3]**
  [Schedule 8 condition 3 DPA]

- **The processing is necessary for: the exercise of a function conferred on a person by an enactment or rule of laws, and: is necessary for reasons of substantial public interest [1]**

[Schedule 8 condition 1 DPA]

- **The processing is necessary for the purposes of: protecting an individual from neglect or physical, mental or emotional harm, or: protecting the physical, mental or emotional well-being of an individual [4]**
  [Schedule 8 condition 4 DPA]

3.2.4 The 6 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 securely 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 Protection Act Principles.

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/right of access requests in compliance with the relevant legislation.

3.3 Statutory Functions

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 s. 251B Health and Social Care Act 2012

This section imposes a duty on the commissioners and providers of healthcare and adult social care to share information with where it is likely to facilitate the provision to the individual of health services or adult social care, and in the individual's best interests.

3.3.5 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 (including NHS bodies) 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.

3.4 Human Rights Act 1998

3.4.1 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.

3.4.2 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 2018, and the minimum necessary to achieve the aims of this agreement, namely, to provide a better service and protection to Adults at Risk.

3.5 Consent

Information can be shared with the consent of the individuals concerned, or without consent in pursuance of public functions, where this is justified in the public interest (or further to statutory obligations). Obtaining consent provides one of the legal bases for sharing

information in compliance with both the Data Protection Act 2018 (above) and the duty of confidence (below). As a matter of good practice, where possible, the Adult at Risk (and any third parties) should be invited to consent to the sharing of information about them, but informed that it may still be necessary to share information without consent.

3.5.1 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), or where seeking consent may prejudice a police investigation or may increase the risk of harm to the Adult at Risk.

3.5.2 Consent can be expressed orally, 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, explicit 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 (therefore, with regard to Schedules 1 and 8, it is preferable to not rely on consent alone wherever possible).

3.5.3 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.

3.5.4 In order to ensure consent to the sharing of personal information is informed, any professional must give victims appropriate information 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 consent.

3.5.5. Professionals should avoid giving absolute guarantees as to confidentiality. 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.

3.5.6 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 (data subject) has previously granted an applicable power of attorney, then it is this appointed person who is able to give consent on the adult's (data subject's) behalf.

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

3.6.1 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 proportion of Adults at Risk whose information may be shared further to this information sharing agreement will lack the mental capacity to make particular decisions about sharing

information (or more generally) 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 is unable to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken, because of an impairment of or disturbance in the mind or brain.

3.6.2 Section 1 of the Mental Capacity 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/she 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[5]
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

3.6.3 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.

3.7 Public Interest

3.7.1 If consent to share 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 interests in safeguarding the Adult at Risk, the provision of confidential services, and the private rights and interests 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.

3.7.2 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?

3.7.3 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?

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

3.7.4 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.

3.7.5 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.

3.7.6 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.

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

3.8 Duty of Confidence

3.8.1 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. Accordingly, much information about Adults at Risk held by Signatory Organisations will be subject to a duty of confidence.

3.8.2 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 publicly known. It has been imparted in circumstances importing an obligation of confidence and its 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.

3.8.3 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.

3.8.4 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.

3.9 Maintaining Confidentiality

As a general rule Signatory Organisations should treat all personal information they acquire or hold in the course of working with Adults at Risk as confidential and take particular care that sensitive information is held securely (in accordance with the protective marking afforded to it by the originating organisation). Anyone who receives information, knowing it is

confidential, is also subject to the duty of confidence. Whenever Signatory Organisations give or receive information in confidence, they 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.

3.10 Fair Processing

Practitioners will normally 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, unless to provide this information would be inappropriate – for instance because it would increase risk unmanageably to the individuals.

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 controller
b) If the 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, Signatory Organisations will have a Fair Processing Notice in place which addresses information sharing for safeguarding purposes and readily accessible for inspection by the public, and this Agreement should routinely be published.

3.11 The Caldicott Principles

The Caldicott Committee's 1997 ***Report on the review of patient-identifiable information***[6] 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. Providers and commissioners of healthcare and adult social care are expected to comply with the Caldicott Principles when sharing information.

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

6) Comply with the law

And additionally, that

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

The Caldicott principles are set out more fully in appendix D below.

3.12 Summary

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

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 organisations 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.

This information sharing agreement has been agreed by all members of the Lambeth Safeguarding Adults Board (April 2019).

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 interests, 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 [7]

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 its: membership; monitoring, development and implementation of its work; training strategy; and planning and implementation of their individual safeguarding assessment and plans.

[7] Safeguarding Adults ADASS, 2005
Metropolitan Police Service (MPS)
Last updated March 2019

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 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 discussed with or disclosed to third parties.

All agencies should ensure that all minutes and related documentation are retained in a confidential manner in accordance with the classification afforded to them.

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 their children;
- 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;
- To reduce repeat victimisation;
- To improve agency accountability; and
- Improve support for staff involved in high risk cases.

Appendix G- Data Protection Act 2018 Six Principles

Principle 1	The first data protection principle states that data must be processed lawfully and fairly.
Principle 2	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Principle 3	Personal data shall be adequate, relevant and limited to the necessities of the purposes for which they are processed.
Principle 4	Personal data shall be accurate and, where necessary, kept up to date.
Principle 5	Personal data must not be kept for longer than is necessary for the purpose for which it is processed.
Principle 6	Personal data shall be processed in a manner that ensures the appropriate security of the personal data.

Appendix H- Sharing Sensitive information by email – guide for health and social care email users

Sharing Sensitive Information by Email –

A guide for Health and Social Care Email Users

February 2019
Version 1

Contents

Purpose of Document

Target Audience: All Health and Social Care Staff using NHSmail

This guidance has been designed to help avoid the use of fax machines or the postal service, to safely and efficiently share personal confidential data and sensitive information where there is a business need to do so by email or Instant Messenger.

A single page summary is included in Appendix 1.

Personal confidential data and sensitive data should be encrypted when sharing by email and assurance sought that the receiver will have appropriate safeguards in place to protect the data upon receipt.

This guide helps senders easily identify which email addresses are known to be secure (protected in transit and upon receipt) and which ones need additional protection when sending personal confidential data and sensitive information.

Summary Guidance

The table below is a summary of email addresses that are known / not known to be secure.

Email to secure addresses are encrypted in transit and the receiving organisation has committed to protect the data upon receipt.

Recipient email address ends	Secure	Additional actions required
*.nhs.net	Yes	Secure – no additional action required
*.secure.nhs.uk	Yes	
*.nhs.uk (does not end secure.nhs.uk)	Unknown	Use [secure] in the subject line
*.gov.uk	Yes	Secure – no additional action required
*. cjsm.net	Yes	
*.pnn.police.uk	Yes	
*.mod.uk	Yes	
*.parliament.uk	Yes	
Any other email address	Unknown	Use [secure] in the subject line

Detailed Guidance

About NHSmail

NHSmail is accredited to the DCB1596 Secure Email Specification and is a secure national collaboration service which enables the safe and secure exchange of personal confidential data or sensitive data within NHSmail and from NHSmail to other suitably accredited email systems. NHSmail also provides the facility to securely exchange information with insecure or non-accredited email services via the NHSmail encryption feature.

All user connections to the service are encrypted. The service operates out of secure, government-rated data centres located in the UK, to provide maximum levels of resilience.

Sending sensitive information to other NHSmail users

Apart from ensuring you have the correct recipient, no additional action or protection is required.

Organisations that use NHSmail have committed to appropriately protect data on receipt as part of their Information Governance obligations.

Note: NHSmail email addresses end with "*.nhs.net".

Sending sensitive information across Health and Social Care

Systems that meet the secure email standard

Locally run email services that meet the secure email standard need no additional action or protection apart from ensuring you have the correct recipient.

Organisations that have met the standard have committed to appropriately protect data on receipt as part of their Information Governance obligations.

Note: These systems have email addresses that end with "*.secure.nhs.uk".

Systems that do not meet the secure email standard

All other "*.nhs.uk" email addresses have not yet met the secure email standard and should not be used for exchanging unencrypted personal confidential data or sensitive data.

Individuals needing to send sensitive information from NHSmail to a "*.nhs.uk" address that does not end with "*.secure.nhs.uk" should use the NHSmail encryption feature.

Note: These systems have email addresses that end with "*.nhs.uk" and do not include .secure.nhs.uk at the end.

Sending sensitive email across Government

Email sent to government email addresses will automatically be sent encrypted to the recipient's email system, providing their system accepts encrypted connections (note all government email services are required to support this).

Any government run email service has a statutory requirement to comply with the Government Security Policy Framework and the Data Protection Act 2018 / General Data Protection Regulation. Where government organisations comply with their statutory requirements, you are assured that the email will be appropriately protected on receipt and not need any additional protection.

Government organisations use a protective marking scheme and NHSmail is suitable for exchanging OFFICIAL and OFFICIAL-SENSITIVE protectively marked information.

The government addresses end with:

*.gov.uk" for local and central government
.cjsm.net" and ".pnn.police.uk" for Police/Criminal Justice
*.mod.uk" for Ministry of Defence *.parliament.uk" for Parliament

Note local and central government historically used legacy email addresses ending with "*.gcsx.gov.uk", "*.gsi.gov.uk" and "*.gsx.gov.uk" which are scheduled for switch off in March 2019. Local and central government organisations will instead switch to using "*.gov.uk" email addresses.

Sending sensitive information to any other system

Note: Any other email address not listed above is not known to be secure.

The NHSmail encryption feature allows NHSmail users to securely exchange personal confidential data with users of non-accredited or non-secure email services. This means users can communicate securely to any type of email account and across the entire health and social care community as well as to patients / citizens.

It is invoked by putting [secure] in the subject line of a message with the inclusion of the square brackets.

Before using the service:

- check local organisation policies and processes on sharing personal confidential data and sensitive information first which will take precedence over this guidance
- ensure you are familiar with the NHSmail Encryption guidance and process

You should only use the NHSmail encryption capability if approved to do so locally.

Receiving sensitive information

Email services that meet the secure email standard and government email services should have been informed by their organisation that it is safe to send personal confidential data to NHSmail without any additional protection.

In line with the NHSmail Acceptable Use Policy and your organisation's Information Governance policies / procedures you will have received guidance and training in how to manage sensitive information and ensure it is protected after receipt.

Electronic and digital signatures

In many instances people need to supply a simple text signature on an email to confirm it has come from them in their official capacity, in the same way they would on a letter or fax. In nearly all cases, ending the email in the same way as you would with a letter is enough:

Name
Job title / role
Organisation

To help avoid forged or spoofed emails where the email has been sent from another email system pretending to be from NHSmail, the service applies technical protections to help avoid this. These include NHSmail informing other email systems of the unique network addresses NHSmail sends its email from and asking them to ignore email if it has come from somewhere else, as well as digitally signing every email sent to let receiving systems know if the content has been tampered with.

Instant Messaging

NHSmail includes an instant messaging service at no additional cost. The exchange of personal confidential data using the instant messenger service is secure but should only be carried out in accordance with your organisation's local Information Governance policies and procedures.

As detailed in the NHSmail clinical safety case, an instant messaging conversation should be treated in the same way as a telephone conversation; after discussing any patient information via this service, users will be expected to properly document a record of all relevant conversations within the patient health record. Local organisations must ensure their staff meet professional standards for clinical documentation following use of the service.

Appendix 1