Title & Version	A purpose specific information sharing agreement between Metropolitan Police Service (MPS) Southwark borough Public Protection Desk (PPD and Missing Persons Unit), Southwark Council Children's Services and Southwark Children's Services ICSS (Integrated Child Support Service) Southwark Education PCT - Version 1
Organisation	Metropolitan Police Service
Summary/Purpose	An agreement to formalise information sharing arrangements between Southwark borough PPD and MPU, Southwark Council Children's Services, Southwark PCT and Southwark Children's Services ICSS (Integrated Child Support Service) for the purpose of identifying and assessing risks to children's wellbeing and welfare in the borough.

ISA Ref: [Insert Gen. Reg Ref]

Purpose Specific Information Sharing Arrangement

Sharing of Police Information by Southwark Public Protection Desk (PPD) and Missing Persons Unit (MPU) to assist in identifying and assessing risks to children's wellbeing and welfare in the borough

Index

Section 1. Purpose of the Agreement

This agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Describe the roles and structures that will support the exchange of information between agencies.
- Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- Describe how this arrangement will be monitored and reviewed. This should be after six months initially and annually thereafter**.**

The signatories to this agreement will represent the following agencies/bodies:

1. **Metropolitan Police Service Southwark borough Public Protection Desk (PPD)**
2. **Metropolitan Police Service Southwark borough Missing Person Unit**
3. **Southwark Council Children's Services - Social Care**
4. **Southwark Children's Services - Integrated Child Support Service (ICSS - who interface with Early Years and Education settings)**
5. **Southwark Primary Care Trust**

Section 2. Specific Purpose for Sharing Information

For many years, the sharing by police of appropriate information about children who come to their notice with local authority social services has been vital in ensuring that as far as is possible the welfare of children is safeguarded. Research and experience has demonstrated the importance of information sharing across professional boundaries.

The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant partner agencies - which include the police, children's' services authorities and Primary Care Trusts - must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act (and rephrased into 'outcomes' in the Government policy 'Every Child Matters') as relating to a child's;

- physical and mental health and emotional well-being ('be healthy')
- protection from harm and neglect ('stay safe')
- education, training and recreation ('enjoy and achieve')
- the contribution made by them to society ('make a positive contribution')
- social and economic well-being ('achieve economic well-being')

The aim of this information sharing agreement is to formally document how Southwark borough police's Public Protection Desk (PPD) and Missing Persons Unit (MPU) will notify Southwark Council Children's Services about children who have come to police notice and are failing at least one of the above five outcomes. It outlines arrangements for any secondary disclosure of MERLIN PAC information by Southwark Council Children's Services, Social Care and Integrated Child Support Service, to Southwark Primary Care Trust, and other agencies.

It will also document how the PPD will respond to requests for information needed to undertake Common Assessment Framework (CAF) on children who have been identified as needing help to achieve one of the five outcomes.

This agreement does not cover the sharing and assessing of police information for use by Southwark Youth Offending Team, nor does it cover referrals made by SCD5 Southwark Child Abuse Investigation Team (CAIT) to the above signatories. These activities will be covered by separate Information Sharing Agreements.

Section 3. Legal Basis for sharing and what Specifically will be Shared

1. First Principle

The first data protection principle states that data must be processed lawfully and fairly.

A public authority must have some legal power entitling it to share the information.

The nature of the information that will be shared under this agreement will often fall below a statutory threshold of S.47 or even S.17 Children Act 1989. If they do fall within these sections of the 1989 Act then these will be the main legal gateway.

However, Sections 10 and 11 of the Children Act 2004 place new obligations upon the police to co-operate with local authorities and other relevant partners such as Primary Care Trusts, in promoting the welfare of children and also ensuring that its functions are discharged having regard to the need to safeguard and promote the welfare of children. This new piece of legislation gives the statutory power to share information for the purposes of this agreement.

Duty of Confidence

Much of the information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children. However, as a safeguard before any information is passed on, it will undergo an assessment check against criteria (included in MPS Safeguarding of Children Standard Operating Procedures) by the Public Protection Desk (PPD). Whilst still applying proportionality and necessity to the decision, the protection of children or other vulnerable persons would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim.

FAIR PROCESSING

The MPS Fair Processing Notice, covering the points specified below, can be found on the MPS website and intranet, is published on the external MPS Publication Scheme and is also displayed within police station front offices and custody suites.

(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 are or are to be processed, to enable processing in respect of the data subject to be fair.

Legitimate Expectation

The sharing of the information by police fulfils a policing purpose, in that it will be done in order to protect life in some circumstances and in others it will fulfil a duty upon the police provided by statute law, (Children Act 2004) i.e. cooperation to improve the well being of children.

It can reasonably be assumed that the persons from whom information is obtained will legitimately expect that police will share it appropriately with any person or agency that will assist in fulfilling the policing purposes mentioned above.

Human Rights - 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.

The sharing of the information with children's services may be in contravention of Article 8. However the benefits of an effective sharing of information for the purposes set out in this agreement are to the direct benefit of the citizen and so in the public interest. This agreement is:

In pursuit of a legitimate aim –

The promotion of the welfare and wellbeing of children and ensuring they achieve all five outcomes is, by virtue of S.11 of Children Act 2004, a major responsibility of the signatories to this agreement and is:

Proportionate –

The amount and type of information shared will only be the minimum necessary to achieve the aim of this agreement, providing a better service to children thus meeting police obligations under the Children Act 2004.

An activity appropriate and necessary in a democratic society –

The police are obliged to do all that is reasonable to ensure the welfare of the most vulnerable of citizens and this is something that is necessary and

appropriate in a democratic society. Primary Care Trusts, Education Authority and Children's Services also have similar obligations, which are necessary and appropriate in a democratic society.

Schedule 2, Data Protection Act 1998

In addition to the legal criteria set out above, the information sharing arrangement must satisfy <u>at least one</u> condition in Schedule 2 of the Data Protection Act in relation to personal data.

Schedule 2 is satisfied in the case of this agreement by condition 5(b) (he exercise of functions conferred under statute) as there is an implied gateway available for the sharing of information in these circumstances under S.11 Children Act 2004, which obliges the relevant agencies to ensure that its "functions are discharged having regard to the need to safeguard and promote the welfare of children".

Schedule 3, Data Protection Act 1998

If the information is "sensitive" (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3.

Schedule 3 is satisfied in the case of this agreement by condition 7, "the processing is necessary for the exercise of any functions conferred on any person by or under an enactment" (i.e. as mentioned above, Children Act 2004).

2. Second Principle

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.

All data that is to be shared is obtained for the purposes of identifying and assessing risks to children. The data is only shared with agencies that are partners with the police in achieving that aim and improving the well being of children.

3. Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The data supplied may consist of:-

- *Name of subject (child) and other family members, their carers and other persons whose presence and/or relationship with the subject child or children, is relevant to identifying and assessing the risks to that child.*
- *Age/date of birth of subject and other family members, carers, other persons detailed.*
- *Ethnic origin of family members.*
- *School (subject only) – not always included.*
- *GP (subject only) – not always included.*
- *Description of incident and police action.*
- *Police checks on all/some family members/ persons mentioned within the Pre-Assessment Checklist (PAC) report.*

Not all of the above information will be shared in every case; only relevant information will be shared on a case-by-case basis where the partner agency has a 'need-to-know' the information.

4. Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

This information comes from MPS corporate systems and is subject to our normal procedures and validations intended to ensure data quality. Any inaccuracies should be notified to the MPS.

Whilst there will be regular sharing of information, the data itself will be 'historical' in nature. Specifically this means that the data fields exclusively relate to individual actions or events that will have already occurred at the time of sharing. These are not categories of information that will substantially alter or require updating in the future.

5. Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The data will be kept in accordance with signatories' file destruction policy. It is acknowledged that there is a need to retain data for varying lengths of time depending on the purpose and also in recognition of the importance of historical information for risk assessment purposes.

6. Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Partners to this arrangement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.

Partners will comply with subject access requests in compliance with the relevant legislation.

The MPS reserves the right to withdraw right of use of the data at any time.

7. Seventh Principle

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.

Measures to satisfy the Seventh Principle are detailed in the Baseline Security Assessment document - prepared as part of the development of this agreement and included in Section Four of the purpose specific agreement, “Description of Arrangements including security matters”

8. Eighth Principle

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

The information is not intended for transfer outside the European Economic Area. Any decision to share the information outside this area would be a matter for the partner agency as long as it is shared within the agreed principles: i.e. for policing purposes, which includes safeguarding children.

Section 4. Description of arrangements including security matters.

MERLIN Pre-Assessment Check (PAC) Notifications

Where it has come to the police's attention that a child is in circumstances that are adversely impacting upon their welfare or safety (i.e. failing at least one of the 5 Every Child Matters outcomes), a Pre-Assessment Checklist (PAC) report will be placed by the reporting police officer on to the MPS system MERLIN.

All police officers and police staff have undertaken Every Child Matters training and the 5 Outcomes associated with the well-being a child. Guidance in relation to when a MERLIN PAC must be created is outlined within the MPS Policy for Safeguarding Children and the accompanying Standard Operating Procedures (SOP).

The Public Protection Desk (PPD) will risk assess each MERLIN PAC. An appropriate level of checks will be completed, using MPS systems, to gain further information on child and 'persons around the child'. The level of police checks that are completed will depend on the category of report. The MPS SOP Safeguarding Children outlines the different categories of report and the levels of checks to be completed for each.

The Public Protection Desk (PPD) will notify the Southwark Council Children's Services where a child has come to the attention of the MPS and it is felt that Children Services have a 'need-to-know[1]' about this incident or the circumstances around the child.

This will be done by sending the PAC report by secure email to the recipient on the Form 87D, which is generated when the PAC form is finalised.

Prior to the PPD sharing any information, a PPD Dedicated Decision Maker (DDM) will review the information in the proposed PAC notification and decide whether or not it is necessary and proportionate to share the information. The DDM will check whether or not the information is accurate, up-to-date and relevant. The DDM will ensure that where the report contains information that is based on opinion or professional judgement, that is clearly identified as being such information.

The DDM will ensure that the Form 87D is sanitised of any information that it is not appropriate to share.

The DDM will then electronically sign the Form 87D to declare that the above supervision has been completed and the report is suitable and ready to be forwarded to Children's Services.

[1] 'Need-to-know': i.e. the minimum information consistent with the purpose for sharing will be given.

The Form 87D will then be sent to dedicated email mailbox at Southwark Children's Services referral and assessment desk. The secure email facility is built into the MERLIN system and uses the Criminal Justice Secure Mail (CJSM) system.

Where the MERLIN PAC relates to a child living on another borough within the MPS district, Southwark PPD will ensure that the PAC is electronically transferred to the relevant PPD or CAIT referral desk responsible for that area. Any sharing of information in relation to that MERLIN PAC will be subject to the local information sharing arrangements between the relevant PPD or CAIT and partners agencies.

Where a MERLIN PAC relates to a child living outside the MPS, the PPD will ensure that the report will be brought to the attention of the appropriate police services' Child Abuse Investigation Team by telephone and then faxing over a copy of the MERLIN entry. Any sharing of information in relation to that MERLIN PAC will be subject to the local information sharing arrangements between that police service and local partner agencies in accordance with ACPO Management of Police Information guidance.

Southwark Children's Services Referral and Assessment Desk (RAD)

Form 87Ds will be received by Children's Services RAD in an email box.

The RAD's Duty Information Officer will be responsible for reviewing all incoming Form 87Ds. This manager will conduct an initial assessment and then allocate the report one of three prioritisation codes: P1, P2 or P3.

Priority 1: Allocation to a social worker for further action. As a general rule these reports are those that relate to a child or family who already have an allocated social worker or contain information that requires a duty social worker to be allocated to conduct further priority enquiries and assessment. The MERLIN PAC will be uploaded onto Southwark Children's Services Care First system.

Priority 2: Further information to be sought to determine whether or not a P1 or P3. This priority code will relate to those reports where the RAD manager, having conducted an initial review of the MERLIN and the Care First system, decides that further checks or enquiries are needed to determine whether or not the circumstances justify a P1 or P3 final categorisation. For example, RAD may make enquiries to ascertain whether or not concerns have been identified by other agencies in relation to the child or family; or whether the child or family are already receiving appropriate support services.

Priority 3: No Further Action by Children's Services/Secondary Disclosure to Partner Agencies. This priority code will be given to those reports where the RAD manager has reviewed the report, the Care First

system and any other relevant information and decided that no further action is required by Children's Services.

Reports falling into this category will also include those where the RAD managers identify issues that they consider another partner agency needs to be aware of in order to ensure that child's wellbeing is safeguarded.

Where the agency concerned is either Southwark Children's Services Integrated Child Support Service (ICSS) where staff including Education Welfare Officers who are linked to schools and early years settings are deployed, or Southwark Primary Care Trust, the RAD manager will undertake secondary disclosure of MERLIN PAC information in strict accordance with the arrangements outlined below.

Where Children's Services identify a need to share MERLIN PAC derived information with any other individual or agency, explicit consent must be first obtained from the Southwark Public Protection Desk.

In Priority 3 cases, the MERLIN PAC will be uploaded onto Southwark Children's Services Care First system or other secure password protected IT system.

Secondary Disclosure of MERLIN PAC Information

Southwark Children's Services (Social Care), Southwark Children's Services (Integrated Child Support Service) and the Southwark Primary Care Trust must obtain the consent of the MPS before making a further disclosure to a secondary body or person i.e. an agency outside this protocol.

Permission must also be obtained before using the information for a different purpose from that which it was first obtained, even if permission has been obtained from the data subject. This is because the further disclosure of police information may have an impact on a policing operation or investigation that the RAD manager is not aware of.

Arrangements

Children's Services Social Care Secondary Disclosure to Children's Services ICSS

Upon receipt and assessment of the PAC notification Children's Services Social Care may identify concerns relating to a child's wellbeing that relate to education issues and/or services.

These concerns are those that relate to any issue that the RAD manager considers that Southwark Children's Services ICSS and education welfare officers and ICSS early years officers have a 'need to know' about in order to fulfil their responsibilities to safeguard the wellbeing of a child.

A Southwark Children's Services ICSS Manager and duty officer are permanently based within the RAD and act as the dedicated single-point-of-contact for all duty enquiries into ICSS.

Where the MERLIN PAC relates to a child of school age, the RAD manager will ask the ICSS Duty Manager or duty officer to check their databases to ascertain whether or not the child is known to Southwark Children's Services ICSS who hold education information about Southwark pupils and whether or not any previous issues relating to the child's well-being have been identified.

Where the RAD manager identifies concerns as outlined above and the relevant child attends a school or early years setting based within Southwark borough, the RAD manager will bring the MERLIN PAC to the attention of the ICSS Duty Manager or duty officer, together with any other relevant information from the Care First system.

The ICSS manager or duty officer will check the details of the child/children concerned against their information systems.

The purpose of these checks will be to (i) confirm which school/early years settings the relevant child attends; (ii) identify whether or not there are any existing concerns or other information relevant to the child's wellbeing and (iii) to identify what, if any, support services the child is already receiving.

Where the education manager or duty worker considers that as a result of the MERLIN PAC information further action is required, they will make a secondary disclosure to the relevant education welfare officer (EWO) or ICSS early years officer.

This secondary disclosure will consist of only that MERLIN PAC derived information which is necessary to allow the education welfare or early years officer undertake the necessary action i.e. the minimum information consistent with the purpose for sharing will be given. This information will include the nominal details of the child and relevant family members or carers.

In the majority cases a simple summary of the concern that has been identified will be sufficient to enable the EWOs or early years officers to perform their role without the need to refer to more detailed information - where it exists - in the report.

Each case requiring disclosure will be assessed by the ICSS duty manager on a case-by-case basis.

Both ICSS and RAD managers will ensure that the information sharing principles of necessity, accuracy and relevance are applied to decision making relating to secondary disclosure.

Both ICSS and RAD managers will ensure that their information systems are updated with a record of what information was disclosed to the EWO or early years officer; the rationale for that disclosure and the MERLIN PAC reference.

Where ICSS or RAD managers are unclear as to the meaning of information within the MERLIN PAC they must contact the PPD.

Pupil's attending schools 'Out Borough' but live in Southwark

Where the RAD manager identifies from a MERLIN PAC an education related concern relating to a child who is schooled on a borough other than Southwark, but lives in the borough of Southwark, the RAD manager will bring the MERLIN PAC to the attention of the ICSS Duty Manager or duty officer, together with any other relevant information from the Care First system in the same way as detailed above.

Where the ICSS Duty Manager considers that as a result of the MERLIN PAC information further action is required, they will make a secondary disclosure to the ICSS 'Out Borough' Education Welfare Officer who is based in Southwark Children's Services ICSS, who will then discuss with the ICSS EWO Manager what information might be shared with an 'Out Borough' school/academy/early years setting that is consistent with the purpose for sharing.

As with pupils educated in Southwark Schools, this secondary disclosure will consist of only that MERLIN PAC derived information which is necessary and will include the nominal details of the child and relevant family members or carers. This information will only be shared with senior members of staff or designated persons for safeguarding in 'Out Borough' Schools/Academies or early years settings.

As with all secondary disclosures highlighted above, both ICSS and RAD managers will ensure that their information systems are updated with a record of what information was disclosed to the EWO or early years officer; the rationale for that disclosure and the MERLIN PAC reference.

Children's Services Secondary Disclosure to Southwark Primary Care Trust (PCT)

Upon receipt and assessment of the PAC notification Children's Services may identify concerns relating to a child's wellbeing that relate to health care issues and/or services.

These concerns are those that relate to any issue that the RAD manager considers that the PCT have a 'need to know' about in order to fulfil their responsibilities to safeguard the wellbeing of a child.

Where the RAD manager identifies such concerns, the manager will produce a simple notification summary of the concern that has been identified. This summary will consist of only that MERLIN PAC derived information which the RAD manager considers necessary to allow the PCT undertake the necessary action i.e. the minimum information consistent with the purpose for sharing will be given. The summary will also contain the MERLIN PAC reference and the

contact number of Southwark PPD. The summary will include the nominal details of the child and relevant family members or carers.

The RAD manager will send the notification summary by secure email (using the CJSM and NHS systems) to the Southwark NHS Named Nurse for Safeguarding (NNS). The email will go into a dedicated email box. Only the NNS and those deputising for the NNS will have access to this email box.

In the majority cases a simple summary of the concern that has been identified will be sufficient to enable the relevant member of PCT staff undertake its responsibilities with regard to safeguarding the wellbeing of children, role without the need to refer to more detailed information - where it exists - in the report.

Each case requiring disclosure will be assessed by the RAD manager on a case-by-case basis.

Children services will not provide MERLIN PAC forms or copies of those forms to NNS without the express permission of a PPD substantive sergeant or above.

The Named Nurse for Safeguarding will review the notification summary and check the relevant nominal details of the child/family against the PCT information systems. The purpose of these checks will be to (i) identify the existence of any concerns or other relevant information with regard to the child's wellbeing; (ii) to identify what, if any, support services the child or family are already receiving and (iii) to identify the need for any further action by the PCT in relation to the wellbeing of children.

The NNS will make a decision as to whether or not any further action is required by the PCT in order to safeguard or promote the wellbeing of the child/children concerned.

Where the NNS identifies that action is required, the NSS will decide what, if any, of the summary of information needs to be passed to a particular member of PCT staff (e.g. a health visitor or midwife) in order for them to effectively take that action. In doing so the NNS will apply the information sharing principles of necessity, accuracy and relevance.

Both the NNS and RAD manager will ensure that their information systems are updated with a record of what information was disclosed; the rationale for that disclosure and the MERLIN PAC reference.

Where NNS or RAD managers are unclear as to the meaning of information within the MERLIN PAC they must contact the PPD to seek clarification.

Secondary Disclosure of MERLIN PAC Information by Southwark Children's Services to non-statutory domestic violence agencies (e.g. BEDE House Association)

Domestic Violence
The police will create a MERLIN PAC in all cases of domestic violence or incidents where children are either present or, if not present at the time, live within the relevant household or where one of the relevant adult parties to the incident is a parent or guardian of a person under 18. All such MERLIN PACs will be sent to Children's Services.

Upon receipt and assessment of the PAC notification Children's Services may identify concerns relating to a child's wellbeing that relate to domestic violence. In order to fulfil their responsibilities to safeguard the wellbeing of a child, Children's Services may identify a need to utilise the specialist domestic violence advice and support services provided by non-statutory agencies.

Where Children's Services identify a need to share information deriving from a MERLIN PAC to such an agency, Children's Services must first obtain the consent of Southwark borough police.

The following process will be followed by Children's Services to seek such consent. Children's Services are to contact the Community Safety Unit Office Management Team via secure email (cjsm.net). All emails are to be sent to the designated email box.

Requesting emails are to contain the following information:

- the MERLIN reference
- detail of the specific information that they wish to share with the domestic violence agency
- which agency they wish the information to be shared with, including the name, telephone number and secure email address of the person(s) to whom the information is to be sent.
- the purpose for sharing that information
- the necessity for sharing that information

The Community Safety Unit (CSU) will review both request and the relevant CRIS reports relating to the domestic violence incident. The CSU will decide whether it is proportionate, relevant and necessary to be disclosed for the purpose requested.

If disclosure is considered appropriate the CSU will send the relevant information to that agency via secure email using the cjsm.net secure email facility, copying in Children's Services. If the relevant agency does not a secure email facility available the information will be sent by fax.

If sending by fax the CSU will check first check that the recipient is on hand to receive it. A cover sheet will be sent first and once confirmation of receipt for this has been received the document containing the information to be shared can then be sent by fax. The requesting officer at Children's Services will be send a copy of the disclosure by secure email.

Note: If disclosure is authorised, it is for the CSU to disclose the relevant information to the relevant agency. The above process will ensure that there is clarity around what information has been or has not been disclosed. The disclosure will be copied in to Children's Services' requesting officer. This will inform any ongoing liaison between Children's Services and the relevant agency.

If the CSU decide that the request for information does not fall within defined categories, the original email request will be returned to the person requesting via secure email. The return email will include an explanation as to why the request did not fall within the defined categories.

Prioritisation of Requests
The CSU Office Management Team (OMT) is staffed Monday to Friday 0800-1800 hours. During that time the OMT will regularly check the email box and ensure that requests are processed in the order that they are received.

Requests will be processed within 24 hours from receipt, with the exception of requests that are received on a Friday in which case Saturday and Sunday will not be counted in that timeframe.

It is vital that the requesting emails contain the information required (above) to avoid delays in this process.

Where Children's Services consider that the circumstances of the case require an urgent disclosure they must, in addition to sending the requesting email, telephone the OMT on the designated telephone number. Outside of OMT office hours, the Duty CSU Detective Sergeant can be contacted between 1800-2200 hours (Monday to Friday) or 0800-1600 hours at weekends.

Where Children's Services are considering making urgent requests outside of normal office hours they must first consider whether or not the agency with whom they wish the information to be shared will have anyone available to receive that information during the proposed timeframe.

Record Management
The CSU will record details of each information sharing request received from Children's Services in relation to domestic violence in accordance with the Management of Police Information (MoPI) standard operating procedure. This will be completed as soon as possible after the information has been shared.

There are two methods available to police to record the sharing of information:

(1) Where there is an 'open' domestic violence CRIS report that is relevant to the case, the information can be recorded on the DETS of that report.
In such cases a copy of the relevant emails/faxes will be filed on division.

(2) In all other cases an 'Information Sharing Record' is to be created on the MPS system CRIMINT Plus. All relevant documents (e.g. emails, faxes) are to be attached electronically to that record.

Resourcing
The CSU OMT is given the central role in the above arrangements due to that unit specialising in the investigation and risk management of domestic violence. This protocol recognises, however, that police operational requirements and resource allocation may necessitate that other officers or units - such as the Public Protection Desk - undertake this role at any one time.

Children's Services Secondary Disclosure to Other Agencies

Where Children's Services identify a need to share MERLIN PAC derived information with any other individual or agency, explicit consent must be first obtained from the Southwark Public Protection Desk.

The only exception to this rule will be where the MERLIN PAC contains within it specific reference by the police to consent to share specific information to another specific agency.

Nothing in section 4 of this arrangement is to be regarded as preventing Southwark Children's Services from taking any necessary urgent action which is critical to preventing a child from suffering significant harm.

Missing Person Notifications & Other Data Sharing

Where a person under 18 years of age is reported missing to the police a MERLIN missing person (MIS) report is completed.

In all cases Southwark Missing Person Unit will send an electronic MERLIN notification to Children's Services via the MERLIN secure email system.

The receipt, assessment and prioritisation of MERLIN MIS notifications will follow the same process as outlined above for MERLIN PACs. With regard to secondary disclosure of MERLIN MIS information by Children's Services with other agencies, the same processes will be followed as outlined above in relation to MERLIN PAC reports.

Police will also periodically provide Southwark Children's Services and the Southwark Council Community Safety Unit with data relating to missing persons. This data may consist of:

- *Name, DOB and gender of the child*

- *Address from which missing*
- *Time/date parameters of the missing episode*
- *Whether or not the child is a Looked After Child*

The purpose of sharing this information is to enable analysis to be undertaken to identify key issues in relation to young people going missing on Southwark borough. In particular, but not exclusively, this will assist the police and Southwark Children's Services identify children who repeatedly go missing with a view to allowing intervention opportunities.

This data will be shared via secure email and will be stored on a password protected system. It will be used only for the purpose provide i.e. analysis.

Information Requests From Partner Agencies to the Police

If Southwark Council Children's Services have concerns about a child, and wish to see if the MPS hold any information relevant to them helping the child, they will complete a request form asking for information and explaining their reasons why (Form 87B - see Annex A). This request form will be sent to via secure email to Southwark SCD5 CAIT Team.

If the request is relating to an SCD5 enquiry, a request for information under Section 17 of Children Act 1989, or refers to an urgent child care placement, then SCD5 will respond directly to the requesting agency.

If the request is needed for the purpose of a Common Assessment Framework (CAF) process, the request will be passed across to the PPD, who will create a new PAC report and look to answer the request.

The PPD will search the appropriate MPS systems including MERLIN, CRIS, CRIMINT Plus, General Registry and also national police systems such as the Police National Computer (PNC) for relevant information. Using the checklist in Form 87C, the PPD will consider the information gathered and decide whether it is proportionate, relevant and necessary to be disclosed for the purpose requested.

If it is decided that the request for information does not fall within defined categories, the original request Form 87B will be returned to the authorising manager via secure email. The return email will include an explanation as to why the request did not fall within the defined categories.

If it 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 the PAC report relating to that request. After removing where necessary any information that is not appropriate to be shared from each report, the PPD will send the finalised answer in the format of Form 87D back to the requesting agency via the secure email facility included within MERLIN and provided by the Criminal Justice Secure Mail (CJSM).

Business Continuity

The mailbox requests and information will be sent to will be a joint team mailbox. Although Children's Services Duty Information Officers will have be responsible for administrating and controlling the mailbox, other appropriate staff within the teams will have access to the mailbox, meaning if the responsible individual is away, work can continue as normal.

The following must be adhered to as a minimum Monday to Friday:

- Team Mailbox is to be checked at the start of the working day between 9am and 10am for all new emails.
- A further check is to be made no later than four hours after the first check.
- A final check is to be made no earlier than 4.30pm.

In the event of a failure of the e-mail system, the above procedures will be applied but the forms will be communicated via fax.

Confidentiality and Vetting

Only staff that have a genuine need to know will be given access to the team mailbox and the information contained within the PAC reports and responses to requests for information.

The information to be shared under this agreement is classified as 'RESTRICTED' under the Government Protective Marking System. Vetting is not mandatory to view this grade of information; however the staff within Southwark Council Child Services, Southwark Primary Care Trust and Southwark Education who will have access to MPS information are CRB vetted. What is required at 'RESTRICTED' level access is a strict 'need-to-know' the information, which all staff viewing PAC reports will have.

Permission must be sought by the partner agencies from the MPS for the sharing of information outside of their respective domain. Such permission will only be granted where proposed sharing is within the agreed principles: i.e. for policing purposes, which includes safeguarding children.

Compliance

All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with.

Any issues concerning compliance with security measures will form part of the annual review of this agreement.

Sanctions

Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of the individual partner.

Non-compliance and/or breaches of the security arrangements will be reported to the Detective Inspector responsible for Southwark police Public Protection Desk and reviewed with regards for any risk in the breach.

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.

Training / Awareness
All partners will hold a copy of this agreement. It is the responsibility of each partner to ensure that all individuals likely to come in contact with the data shared under this agreement are trained in the terms of this agreement and their own responsibilities.

Partner's Building And Perimeter Security
Information will be stored in secured premises, e.g. not in areas where the public have access.

Movement of Information (Electronically).
As mentioned previously, requests for information and responses to those requests will be sent electronically via secure email to group email inboxes. These email inboxes are all considered secure due to the network they sit on; PPD mailbox is on the Police National Network (pnn), the Council is part of the Criminal Justice Secure Mail (CJSM) network and PCT nhs.net email address is consider safe to the same standards as the pnn and cjsm networks.

Storage of Information on Partner's System
As mentioned previously, information will be sent via secure email to a joint mailbox. Information within the email will be stored there and then transferred to the appropriate electronic system within five days of the email being received. The email will then be deleted.

Signatories to this agreement confirm that there are adequate security measures on their electronic systems that information from partners may be transferred to. Information can only be accessed via username and password. Partners confirm that permission to access to MPS information held electronically by partners will be granted on a strict 'need-to-know' basis once it is contained within partners' electronic systems.

Storage of Papers
It is not the intention of this agreement that information will be produced in a hard format. If information is printed off of an electronic system, it will be the partners' responsibility to keep the information secure by measures such as storing documents in a locked container when not in use. Access to printed

documents must be limited only to those with a valid 'need to know' that information. There should also be a clear desk policy were MPS information is only assessed when needed and stored correctly and securely when not in use.

Disposal of Electronic Information
Once information contained within emails is transferred to partner's electronic systems, the emails will be deleted.

Information will be held in electronic systems until the information is no longer required. Information provided as part of this agreement will be the subject of review by the partner agencies. Information will be destroyed in accordance with each agencies code of practice in handling information and with regards to their responsibilities under the Data Protection Act.

If information is stored by partners electronically on their systems, information must be overwritten using an appropriate software utility e.g. Norton Utilities or CD discs physically destroyed

Disposal of Papers
As mentioned previously, it is not the intention of this agreement that information will be produced in a hard format. If information is printed off of an electronic system, it will be the partners' responsibility to dispose of the information in an appropriate secure manner (i.e. shredding, through a 'RESTRICTED' waste system) once it is no longer needed.

Review
The arrangements held within this document will be reviewed initially after six months and then annually thereafter

Freedom of Information Requests
This document and the arrangements it details will be disclosable for the purposes of the Freedom of Information Act 2000 and so will be published within the signatories' Publication Schemes.

Any requests for information made under the Act that relates to the operation of this agreement should, where applicable, be dealt with in accordance with the Code of Practice under S.45 Freedom of Information Act 2000.

This 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 also transfer all or part of a request to another authority if it relates to information they do not hold.

Section 5. Agreement to abide by this arrangement

The agencies signing 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 procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners initially after 6 months from signature then at least annually.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date
Metropolitan Police Service, Southwark borough				
Southwark Council Children's Services - Social Care				
Southwark Primary Care Trust				
Southwark Council Children's Services - ICSS				