INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Thurrock Multi Agency Safeguarding Hub (MASH): Guide to Information Sharing Agreement and Guidance document 2019

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Thurrock Children Services	Thurrock Council, Civic Offices, New Road, Grays, Essex RM17 6SL	01375 652500	lhenley@thurrock.gov.uk	Lee Henley	Z8228055

See Appendix for all signatories

Version Control	
Date Agreement comes into force	2nd September 2019
Date of Agreement review	2nd September 2020
Agreement owner (Organisation)	Thurrock Council
Agreement drawn up by (Author(s))	Joseph Tynan Strategic Lead Thurrock
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	V: 2

Please ensure all sections of the template are fully completed with sufficient detail to provide assurance that the sharing is conducted lawfully, securely and ethically.

Item	Name/Link /Reference	Responsible Authority
Privacy Impact Assessment (PIA/DPIA)		A DPIA has not been completed retrospectively, this is a well-established initiative which has not been the subject of complaint or data breach. A DPIA will not be undertaken until circumstances significantly change
Supporting Standard Operating Procedure		
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the WEISF Portal.

1.	Purpose	REFERENCES

This agreement:

Forms the basis for the lawful sharing of information between signatories organisations involved in the safeguarding of children.

- Facilitate the exchange of personal and sensitive information in the interests of protecting children and young people from actual or potential harm and to ensure that when information is shared the legal means to do so exists.
- Provide early and effective multi-agency intervention to safeguard children and young people with care and support needs, which will promote social inclusion, health and well-being.
- To encourage and help develop effective information sharing between different services and professionals groups, based upon trust and mutual understanding.
- Facilitate and provide clear guidance on the exchange of personal and sensitive information for the investigation and response to suspected abuse and neglect of children and young people in Thurrock

under the Safeguarding Children procedures.

SET Safeguarding and Children Protection Procedures

Introduction

In order to ensure that safeguarding decisions are made in a timely manner, necessary and proportionate interventions, and decision-makers requires full information concerning an individual and their circumstances. Information viewed alone or in siloes is unlikely to give the full picture or identify the risk.

All relevant information from various agencies needs to be available and accessible in one place. A Multi Agency Safeguarding Hub (MASH) helps ensure this and aids communication between all safeguarding partners, thus ensuring that the team quickly identifies those who are subject to or at risk of harm.

Information should only be shared within the MASH for the purposes of safeguarding and promoting the welfare of children, and for the prevention and detention of related crime.

HM Government advice on Information Sharing (March 2015) states that:

"Sharing information is an intrinsic part of any front-line practitioner's job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death."

Poor or non-existent information sharing is a factor repeatedly flagged up as an issue in serious case reviews (SCR) carried out following the death or serious injury to a child.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. No practitioner should assume that someone else will pass on information which may be shared with or without consent, through considering what is reasonable, necessary and proportionate.

The Children Act 2004 emphasizes the importance of safeguarding children by stating that relevant partner agencies - which include the police, children's services authorities, Clinical Commissioning Groups and the NHS England - 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 as relating to a child's:

1. Physical and mental health and emotional well-being ('be healthy')
2. Protection from harm and neglect ('stay safe')
3. Education, training and recreation ('enjoy and achieve')
4. The contribution made by them to society ('make a positive contribution')
5. Social and economic well-being ('achieve economic well-being')

Although most commonly used to refer to young people aged 16 or under, 'children' in terms of the scope of this Act means those aged eighteen or under.

Section 2. Specific Purpose for Sharing Information

MASH helps deliver three key functions for the safeguarding partnership;

1. Information based risk assessment and decision making
Identify through the best information available to the safeguarding partnership those children and young people who require support or a necessary and proportionate intervention.

2. Victim identification and harm reduction
Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions.

3. Co-ordination of all safeguarding partners
Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and co-ordination of harm reduction strategies and interventions.

The MASH model was highlighted in the Munro Report into Child Protection (http://www.education.gov.uk/munroreview/downloads/8875_DfE_Munro_Report_TAGG_ED.pdf) as an example of good practice in multi-agency partnership working because of how it improved information sharing between participating agencies.

The aim of this information sharing agreement is to document how through the MASH set-up the signatories to this agreement will share information about children who have come to attention for being at risk of failing to achieve at least one of the five outcomes listed above on the previous page.

This agreement does not cover other information sharing between the signatory agencies that take place outside of the MASH. These transactions will be covered (where appropriate) by separate information sharing agreements.

The seven golden seven rules to sharing information

1. Remember that the Data Protection Act 2018 and Human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners if you are I doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent if, in your judgment, there is a good reason to do so, such as where safety may be at risk. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to he shared.

5. Consider safety and well: Base your information sharing decisions on considerations of the safety and well-being of the individuals and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles)

7. Keep a record of your decision and the reasons for it, whether it is to share information or not. If you decide to

share, then what you have shared, with whom and for what purpose.

Definitions

Personal Information/Data is:

- Information/Data which relates to a living, individual who can be identified from the date or other date/information that Thurrock holds.
- Could be single elements or a combination e.g. names, addresses, occupation, date of birth etc. it could also include opinions about them and intentions towards them.

Special Categories of personal data are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Health data
- Sex life or sexual orientation

Principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers. Practitioners should use their judgment when making decisions on what information to share and when and should follow organization procedures or consult with their manager if in doubt. The most important consideration is whether sharing information is likely to safeguard and protect a child.

Necessary and Proportionate

When taking decisions about what information to share, you should consider how much information you need to release. The Data Protection Act 2018 requires you to consider the impact of disclosing information on the information subject and any third parties. Any information shared must be proportionate to the need and level of risk.

Relevant

Only information that is relevant to the purpose should be shared with those who need it. This allows others to do their job effectively and make sound decisions.

Adequate
Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate
Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely
Information should be shared in a timely fashion to reduce the risk of harm. Timeliness is key in emergency situation and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm a child. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure
Information should be shared in the most secure way available. Practitioners must always follow their organisation's policy on security for handling personal information.

What information can I Share?

Share the information which is necessary for your purpose. It may not be necessary to give all agencies access to all information you hold. Make sure what you provide is up to date, accurate and relevant.

When and how to share information
When asked to share information, you should consider the following questions to help you decide if and when to share. If the decision is taken to share, you should consider how best to effectively share the information.

When?

Is there a clear and legitimate purpose for sharing information?

- Yes –see next question
- No-do not share information

Does the information enable an individual to be identified?

- Yes-see next question
- No-you can share but should consider how

Is the information confidential?

- Yes-see next question
- No- you can share but should consider how

Do you have consent?

- Yes-you can share but consider how
- No- see next question

Is there another reason to share information such as to fulfil a public function or to protect the vital interest of the individual?

- Yes-you can share but consider how
- No- do not share

Who?

- Which agencies need to be involved in the sharing?
- Who do we need information about in order to make the decision-child, parent, carers, others? Is it sensitive personal information? Do we have their consent?

How?

- Ensure you are giving the right information to the right person, and that it is shared securely.
- Identify how much information to share
- Distinguish fact from opinion

Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm.

2.	**Information to be shared**	

We will share information relevant to safeguarding as allowed by the legislation. The following are examples information to be shared, **but it should be noted that the sharing relates to all multi-agency safeguarding groups, and not only those noted below.**

- 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.
- Relevant Police information and intelligence
- Information that will contribute to an assessment to enable workers to complete a holistic assessment of a child and family
- Information exchanged for the purposes of risk management via Multi-agency Public, Protection Arrangements (MAPPA), such as data relating to convictions, cautions, final warnings, reprimands, details of case histories and intelligence, if appropriate, to the subject person
- Information required to manage risks and formulate safety plans for victims and their families in Thurrock via the Local Safeguarding Children's Board
- Information about the risk posed by people who are convicted of offences against children and vulnerable offenders
- Information as required for Child Death Overviews Panels and the Child Death Review process
- Information required for safeguarding reviews such as Serious Case Reviews (SCR) and Partnership Learning Reviews
- Information required for Multi-agency Risk Assessment Conference (MARAC)
- Datasets and information required for Thurrock's Child Exploitation Panel (MACE). Including information on potential suspects or person/s of concern linked to a child sexual exploitation and hot spots. The collation of data in the support of patterns or trends and early identification and trafficking
- Information sharing to support the prevent strategy
- Data Required to meet any inspections regimes, timescales and request; data required as part of the work on the Health and Social Case prevention agenda:
    1. Child's name, address, gender, date of birth, and a minimum, educational setting (e.g. school)
    2. Contact details for parents/carers;
    3. Contact details for services working with a child: as a minimum (educational setting (e.g. school) and GP practice, but also other services where appropriate;
    4. Type and details of concerns and case information;
- Detains of Family Support Meetings

- School and educational information (to include family members where appropriate and relevant)
- GP and health records (to include family members where appropriate and relevant)
- Relevant ASB data
- Relevant data from London Ambulance Service or London Fire Brigade
- Housing and other partnership data relevant to the child and family who may affect the welfare of that child.

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 an organisation has a 'need-to-know' about the information.

3. Legal Basis

General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.

GDPR
Go to articles 6 and 9

Personal Data (identifiable data)	Special Categories of Data (Sensitive identifiable data)
Article 6: ***[please click and select]***	Article 9: (if appropriate): ***[please click and select]***
Legal Obligation	Substantial Public Interest
Public Task	Health & Social Care
Choose an item.	Vital Interests

HM Government has published guidance which should be read in conjunction with this agreement and it is an invaluable resource for all safeguarding professionals working with children, young people and families;

1. Information sharing: Advice for practitioners providing safeguarding services 2018
https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

The document should be considered as an accurate summary of legal principles and of what the law requires for

decision making to be lawful concerning the sharing of information and not merely, as guidance.

Local authorities responsibilities for sharing information under the Care Act 2014

Under the Care Act 2014 a local authority must:

- Set up a safeguarding board; the board will share strategic information to improve local safeguarding practice
- Co-operate with each of its relevant partners; relevant partners must cooperate with the local authority.

For Parties responsibility the following apply:

1. The use of confidential information or any part of it only for the purpose expressly set out in the agreement
2. Organisational and security measures to protect the lawful use of information shared under this agreement
3. Procedures in place to address complaints relating to inappropriate disclosure

The Caldicott principles

The sharing of information in health and social care is guided by the Caldicott principles. These principles are reflected in the Data Protection Act 2018 and are useful to other sectors:

- Justify the purpose(s).
- Don't use personal confidential data necessary for purpose.
- Use the minimum personal confidential data necessary for purpose.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

Relevant legislation when sharing specific information relating to children are:

1. The Children Act 1989 and 2004
2. The Childcare Act 2006
3. The Education Act 2002
4. Learning and Skills Act 2000
5. Children (leaving care) Act 2000
6. Protection of Children Act 1999

7. Local Government Act 2000
8. Criminal Justice Act 2002
9. Data Protection Act 2018

2. Attention is drawn in addition to the **'seven golden rules'** set out in the Information sharing: Advice for practitioners providing safeguarding services 2018 as a practical exposition of the law relating to information sharing.

For the protection and use of personal information the following guidance is available:

1. Human Rights Act 1998
2. The Common Law Duty of Confidence

The SET Procedures should also be viewed as useful guidance in this area.
https://www.thurrocklscp.org.uk/lscp/professionals/set-procedures

The Data Protection Act 2018 identifies 6 key principles in relation to the sharing of personalised data.

1. First Principle[1]

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.

Some concerns regarding children where information will need to be shared under this agreement will often fall below a statutory threshold of Section 47 or even Section 17

Children Act 1989. If they do however fall within these sections of the 1989 Act then these sections will be the main legal gateway.

Sections 10 and 11 of the Children Act 2004 place new obligations upon Local authorities, police, clinical commission groups and the NHS England to co-operate with other relevant partners in promoting the welfare of children and also ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

Section 10 and 11 of the Children Act 2004 create a 'permissive gateway' for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information namely the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law duty of confidentiality.

Schedule 2 part 1 para 2 (1) of the Data Protection Act 2018 allows data to be shared without consent if it is relation to the prevention or detection of crime or the apprehension or prosecution of offenders.

Under this agreement, if not disclosing information to the MASH would prejudice the situations listed above, organisations are then exempt from the usual non-disclosure provisions and may provide the information requested / they wish to share proactively.

All decisions to share or not share information **must** be decided on a case-by-case basis and recorded.

Duty of Confidence

A duty of confidence may be owed to both the holder of the data and to the data subject. Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children. However, as a safeguard before any information is passed on, police information will undergo an assessment check against set criteria by Essex Police within the MASH.

[1] In accordance with the Data Protection Act 2018

Whilst always applying the tests of proportionality and necessity to the decision to share information, 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. All information shared with a partner agency must be relevant to the case in point.

Information held by other agencies that will be shared in the MASH may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure, as information can be shared where consent has been provided or where there is a strong enough public interest to do so as it relates to the wellbeing of children, young people and their families.

Consent

The starting point in relation to sharing information is that practitioners will be open and honest with families and individuals from the outset about why, what, how and with whom information will or could be shared.

It may be necessary and desirable to deviate from the normal approach of seeking consent from a family in cases where practitioners have reasonable grounds for believing that asking for consent would be unsafe or inappropriate. There must be a proportionate reason for not seeking consent and the person making this decision must try to weigh up the important legal duty to seek consent and the damage that might be caused by the proposed information sharing on the one hand and balance that against whether any, and if so what type and amount of harm might be caused (or not prevented) by seeking consent.

There is no absolute requirement for agencies in the MASH to obtain consent before sharing information nor there a blanket policy of never doing so. There is an obligation to consider on all occasions and on a case by case basis whether information will be shared with or without consent. This determination by a practitioner should always be reasonable, necessary and proportionate in line with the seven golden rules of information sharing. It should always be recorded together with the rationale for the decision.

Section 47 Thresholds do not determinate whether or not consent should be sought within MASH.

It is inherent in the idea of seeking consent that it will be refused. If professionals consider it justifiable to override the refusal in the interests of the welfare of the child then they can and must do so. This decision must be proportionate to the harm that may be caused by proceeding without consent.

Where it is believed the aims of the MASH might be prejudiced if agencies were to seek consent the disclosing agency must consider the grounds to override the consent issue.

The disclosure of personal information without consent is legally justifiable if it falls within one of the defined category of public interest:

The Public Interest Criteria include:

i) The administration of justice;
ii) Maintaining public safety;
iii) The apprehension of offenders;
iv) The prevention of crime and disorder;

v) The detection of crime;
vi) The protection of vulnerable members of the community.

When judging the public interest, it is necessary to consider the following:

i) Is the intended disclosure proportionate[2] to the intended aim?
ii) What is the vulnerability of those who are at risk?
iii) What is the impact of disclosure likely to be on the individual?
iv) Is there another equally effective means of achieving the same aim?
v) Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public;
vi) Is it necessary to disclose the information, to protect other vulnerable people?

As previously stated a proportionality test must be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

Information is shared initially within the MASH with or without consent in order to assess risk and harm which in turn identifies the proportionate level of response required. If information is disclosed with or without consent, it is essential that there is a clear record of the reason and justification for disclosure, so as to demonstrate that the decision is reasonable, proportionate and justified.

Once a decision is made based on this shared information picture the local authority decision maker together with the relevant partner may hold back within the MASH any information which is deemed by the originating organisation to be too confidential for wider dissemination. Should it be decided to retain confidential information within the MASH then it will always be sign posted to any professional who may receive a referral or request for service.

When overriding the duty of confidentiality the MASH must seek the views of the organisation that holds the duty of confidentiality and take into account their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

The MASH processes if followed correctly are relevant in relation to the determination of consent. The MASH comprises a relatively closed and controlled environment, this being a factor a practitioner can weigh in the balance to some extent in an appropriate case as one factor that can add to the conclusion that it is proportionate not to seek or to dispose with consent. It is not however a single overriding reason in the determination concerning consent.

All disclosures must be relevant and proportionate[3] to the intended aim of the disclosure.

[2] "Proportionate" is the critical issue.
[3] The implication here is that full records should not be routinely disclosed, as there will usually be information that is not relevant

Unified Privacy[4]

It is a requirement of the Data Protection Act 2018 that all organisations that process personal data should have what is now known as 'Unified Privacy Notice' which will inform individuals about how their personal data will be used by that organisation. This notice will cover:

(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.

The local authority will publish a Unified Privacy Notice specifically identifying the MASH within it and partner organisations will all publish a Unified Privacy Notice in their normal manner. In Regards to Police personal information, this will be used for the purposes of 'Policing' and the notices states that information may be shared with a variety of other agencies for the purposes of Policing.

If staff of signatory agencies receives information and they believe that by NOT disclosing this information the police will be unable to prevent or detect a crime, or the police will be unable to apprehend or prosecute an offender, then they may fairly share that information with the police. This decision will be taken on a case-by-case basis and recorded.

Legitimate Expectation

The sharing of the information by partners fulfil a duty upon them provided by statute law (Children Act 2004) i.e. co-operation to safeguard or promote the wellbeing of children. (Section 10 and Section 11)

For police 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.

As previously identified consent will have been considered before the individual's case is brought to the MASH. In cases, where consent has been granted individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why.

[4] Previously known as; 'fair processing'.

Human Rights Act 1998 - 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.

Consent is relevant to the rights of those to whom confidential information relates, and thus to legal obligations such as the Human Rights Act 1998.

The sharing of information with children's services may engage Article 8 however there will be no contravention provided that an exception within Article 8(2) applies.

The benefits of effective sharing of information for the purposes set out in this agreement are to the direct benefit[5] of the citizen and so in the public interest. This agreement is:

<u>In pursuit of a legitimate aim</u> –

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 legitimate aim and major responsibility of the signatories to this agreement. The sharing of information under this agreement is also in line with Articles 2 and 3 of the Human Rights Act 1988, namely the right to life and the right to prohibition of torture or inhuman or degrading treatment.

<u>Proportionate</u> –

The amount and type of information shared will only be that necessary to achieve the aim of this agreement. Information is always to be considered in terms of its proportionality in each set of circumstances, but it must

always be remembered that the right to life is paramount.

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. Other signatories to this agreement such as Clinical Commissioning Groups and Children's Services also have similar obligations, which are necessary and appropriate in a democratic society.

2. Second Principle

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

The Police information exchanged under this agreement was obtained for policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose. Likewise, other agencies also collect information for other purposes

All information will only be used within the MASH for the purposes of safeguarding the vulnerable and reducing harm, which is not incompatible with the reason it was originally collected.

3. Third Principle

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Due to the complexity of the MASH, providing a prescriptive list of data fields to be shared is difficult.

Any information that is shared into and within the MASH Hub will be decided on a case- by-case basis and must be relevant to the aims of this agreement.

4. Fourth Principle

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

All the information supplied will be obtained from signatories' computer systems or paper records and subject to their own organisations reviews, procedures and validation. Any perceived inaccuracies should be reported to the contact at that agency for verification and any necessary action.

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. The exception to this will be that of the unborn child.

5. Fifth Principle

Personal data shall be kept in a form which permits identification of data subjects for no longer than necessary

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. However, once information is no longer needed, it should be destroyed.

6. Sixth Principle

Personal data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss or destruction

Measures to satisfy the Sixth 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"

Other legislation and guidance

Information regarding the high risk of domestic abuse may be shared under the following legislation:

- Children Act 1989/2004

- Articles 2 and 3 of the Human Rights Act 1998
- Equalities Act 2010
- Section 115 Crime and Disorder Act 1998
- Section 120 Learning and Skills Act 2000
- Section 325 Criminal Justice Act 2003 (Duty to co-operate)
- Sections 39 and 39a police Act 1996 (Code of practice on the Management of Police information)

In March 2015, the government issued a report on **Tracking Sexual exploitation, along with a letter on our joint commitment to share information effectively for the protection of children.**

4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as follows: For help go to https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN Articles 24 – 29 where these roles are explained.	Tick box	Organisation Name(s)
The Data Controllers for this sharing are:	☒	See Signatories
The Joint Data Controllers for this sharing are:	☐	
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is: Joe Tynan - Strategic Lead	☒	Thurrock Council
Data Processors party to this protocol are (please list):	☐	

This Protocol will be reviewed one year after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by Joe Tynan Strategic Thurrock Council Lead.

5. Subject Rights

Essex Partner Agencies' Information Sharing Agreements are made publicly available on the WEISF website to enable compliance with article 12 of the GDPR.

It is each Partner's responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	Processes are in place to enact this right - please check the box
GDPR Article 13&14 / DPA 2018 (44) – **Right to be Informed** – Individuals must be informed about how their data is being used. This sharing must be reflected in your privacy notices to ensure transparency.	☐
GDPR Article 15 / DPA 2018 (45)– **Right of Access** – Individuals have the right to request access to the information about them held by each Partner	☒
GDPR Article 16 / DPA 2018 (46) – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	☒
GDPR Article 17 (1)(b)&(e) / DPA 2018 (47) – **Right to be forgotten** – This right may apply where the sharing is based on Consent, Contract or Legitimate Interests, or where a Court Order has demanded that the information for an individual must no longer be processed. Should either circumstance occur, the receiving Partner must notify all Data Controllers party to this protocol, providing sufficient information for the individual to be identified, and explaining the basis for the application, to enable all Partners to take the appropriate action.	☒
GDPR Article 18 / DPA 2018 (47) – **Right to Restriction** – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☒
GDPR Article 19 / / DPA 2018 (44) – **Notification** – Data Controllers must notify the data subjects and other recipients of the personal data under the terms of this protocol of any rectification or restrict, unless it involves disproportionate effort.	☒
Article 21 – **The Right to Object** – Individuals have the right to object to any processing which relies on Consent, Legitimate Interests, or Public Task as its legal basis for processing. This right does not apply where processing is required by law (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☒
Article 22 / DPA 2018 (49) – **Automated Decision Making including Profiling** – the Individual has the right to request that a human being makes a decision rather than a computer, unless it is required by law.	☒

Freedom of Information (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 relates to data requested from a Public Authority by a member of the public. It is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption/exception and to identify any perceived harms. However, the decision to release data under the FOI Act or EIR is the responsibility of the agency that received the request.	☒	

6. Security of Information

Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
Paper information is stored securely	☒	
Paper and electronic information is securely destroyed with destruction log for electronic information	☒	
Laptops and removable media such as memory sticks are secured when not in use	☒	
Technical security appropriate to the type of information being processed is applied	☒	
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	☒	
Disaster recovery arrangements are in place	☒	
Encryption of personal data is fully implemented	☒	
Data minimisation has been considered	☒	
Can pseudonymised or anonymised data be used to meet your processing needs?	☒	
There are sufficient access controls for systems/networks in place	☒	
Routine and regular penetration tests are carried out	☐	
Article 40 Codes of Conduct are adhered to (where applicable)	☐	
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	☒	
Confirm entry in Records of Processing Activity	☒	
Additional measure 1 – please specify here	☐	

Additional measure 2 – please specify here	☐

Personal information will be securely shared via Email, telephone or post etc. Members are to ensure that their local procedures surrounding secure methods of data transfer are followed their should include the following:

- When disclosing information by telephone consideration must be given to authenticating the caller and ensuring sensitive conversations are overheard.
- Do not send personal or confidential information to person email address.
- Information I hard copy format send via royal mail must be double wrapped
- If the Data is particular sensitive partners may wish to consider using special delivers or a contracted currier under track conditions
- Information send in hard copy must be address to a person 'address only'
- If information is to be sent via Fax then safe haven procedures must be used.

Partners receiving information will:

- Ensure that their employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
- Protect the physical security of the shared information;
- Restrict access to data to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks
- Maintain an up to date policy for handling personal data which is available to all staff
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

International Transfers (Where applicable)

If any personal data is to be transferred outside of the EEA, please ensure you capture the relevant supporting adequacy decision for such a transfer here in line with Article 46. .

7. Format and Frequency

The format the information will be shared in is by secure electronic method. Information will be stored securely on the LCS / EHM

database, e.g. not in areas where the public have access.

Movement of Information

Information will be sent and received electronically to ensure there is an audit trail of its movement.

Any e-mail communication will be by way of secure, appropriate and approved methods. The sharing of information must be done via secure email. Thurrock Council's email system adheres to the Government requirement of TSL v1.2 and therefore emails can be exchanged using a thurrock.gov.uk address securely. Other secure domains (this is not an exhaustive list) includes pnn & nhs.net. Emails to these domains do not require any additional level of security or encryption.

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 an electronic system by the individuals in the MASH, it will be the owner's responsibility to dispose of the information in an appropriate secure manner i.e. shredding or through a 'SECURE' waste system, once it is no longer needed.

The frequency with which the information will be shared, the format and frequency will all depend upon the circumstances in which the information is being shared. Data will be shared regularly as required for the purpose specified sharing.

- Requirement of the Thurrock Safeguarding Children board
- Any inspection regimes, timescales and request in addition, some anonymised (or pseudonymised) information will only be released at certain points in the year to prevent individuals being identified.

8. Data Retention

GDPR
Go to article 5

Information will be retained in accordance with each partners' published data retention policy available on their websites, and in any event no longer than is necessary.

The MASH enquiry records will be stored on the LCS / EHM system.

However, other agencies may be passed information from the MASH case record where appropriate for further interaction with a child, which may also be stored electronically.

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 an electronic system, it will be the partner's 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 and particular information from any agency 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

9. Data Accuracy

Please check this box to confirm that your organisation has processes in place to ensure that data is regularly checked for accuracy, and any anomalies are resolved ☒

GDPR
Go to articles 5, 16 - 18

10. Breach Notification

Where a security breach linked to the sharing of data under this protocol is likely to adversely affect an Individual, all involved Partners must be informed within 48 hours of the breach being detected. The email addresses on Appendix 1 should be used to contact the Partners. The decision to notify the ICO can only be made after consultation with any other affected Partner to this protocol, and notification to the ICO must be made within 72 hours of the breach being detected. Where agreement to notify cannot be reached within this timeframe, the final decision will rest with the Protocol owner as depicted on page 1 of this document.

All involved Partners should consult on the need to inform the Individual, so that all risks are fully considered and agreement is reached as to when, how and by whom such contact should be made. Where agreement to notify cannot be reached, the final decision will rest with the Protocol owner as depicted on page 1 of this document.

GDPR
Go to articles 33, 34, 77 - 84

All Partners to this protocol must ensure that robust policy and procedures are in place to manage security incidents, including the need to consult Partners where the breach directly relates to information shared under this protocol.		
11.	**Complaints**	
Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.		GDPR Go to articles 16 – 22 & 77
12.	**Commencement of Protocol**	
This Protocol shall commence upon date of the signing of a copy of the Protocol by the signatory partners. The relevant information can be shared between signatory partners from the date the Protocol commences.		
13.	**Withdrawal from the Protocol**	
Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the Thurrock Council, GCThurrockMash@thurrock.gcsx.gov.uk The Team Manager of MASH will notify other Partners to the Protocol. The Partner must continue to comply with the terms of this Protocol in respect of any information that the partner has obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate secure manner.		
14.	**Agreement**	

This Protocol must be approved by the responsible person within the organisation (SIRO/Caldicott Guardian/Chief Information Officer).

Approver Name	Lee Henley
Organisation Name	Thurrock Council
Date of Agreement	2nd September 2019
Name of Departmental Lead and Job Title	Joe Tynan, Children's Care, Care and Targeted Outcomes Team Manager

Approver Name	Mark Madden
Organisation Name	Essex Partnership University NHS Foundation Trust
Date of Agreement	14.04.2020
Job Title	SIRO

Approver Name	Dr Milind Karale
Organisation Name	Essex Partnership University NHS Foundation Trust
Date of Agreement	14.04.2020
Job Title	Caldicott Guardian

Please submit this Protocol to information.matters"thurrock.gov.uk with list of approved signatories. The Protocol will then be published

Email approvals will only be accepted from an authorised signatory role from each organisation. Please see the list of authorised roles per organisation on Thurrock Council's website

15. Agreement to abide by this arrangement

Agreement Title: **Thurrock Multi Agency Safeguarding Hub (MASH): Guide to Information Sharing Agreement and Guidance document 2019**

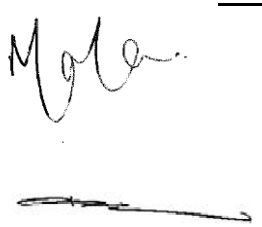
Signatories of this agreement must accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities. As such they must:

- 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:

Organisation Name	
ICO Reference	
Name	
Post Held	
Email Address	
Signature	
Date	

Appendix 1

Name of organisation	ICO reference	Name of signatory	Job title	Email address	Signature	Date signed
Thurrock Council	Z8228055	Lee Henley	Strategic Lead – Information Management	lhenley@thurrock.gov.uk		02/09/2019
Essex Partnership University NHS Foundation Trust	ZA242481	Mark Madden Dr Milind Karale	Senior Information Risk Owner (SIRO) Caldicott Guardian	**epunft.info.gov@nhs.net**		14.04.2020