Enfield Safeguarding Children Board
...because safeguarding children is everybody's business

INFORMATION SHARING PROTOCOL

ENFIELD Children's Social Care

Incorporating a Multi-Agency Safeguarding Hub (MASH)

Author(s)	Sarah Moran, Head of Service MASH, Assessment & EDT Antony Demetriou, MASH Team Manager	Classification	**OFFICIAL - PUBLIC**	Date of First Issue	2013
Owner	Anne Stoker, Assistant Director Children's Social Care	Issue Status	**Final**	Date of Latest Re-Issue	June 2018
Governance	Agreed at DMT on 6/6/18 Ratified by ESCB on 18/6/18		**Final**	Date of latest Issues	June 2018
Version	**3.0**	Page	Page **1** of **27**	Date of Next Review	June 2019

Contents

1. Executive Summary

"Early sharing of information is the key to providing effective early help where there are emerging problems. At the other end of the continuum, sharing information can be essential to put in place effective child protection services. Serious Case Reviews (SCRs) have shown how poor information sharing has contributed to the deaths or serious injuries of children." - Working Together to Safeguard Children (2015)

1.1 This document is an overarching information sharing protocol for inter-agency information sharing within Enfield. It is designed to support effective communication between professionals and will ensure better understanding of what information should be shared, with whom and under what circumstances, and the dangers of not doing so.

1.2 It is always better to work in partnership with children & their families and where possible consent to share information can and should be sought. Where there are no safeguarding concerns you should always seek to obtain consent. However, consent should not act as a barrier to sharing information where there **are safeguarding concerns** about a child. Enfield is committed to ensuring that children & their families are supported and protected at the earliest opportunity and that this important work is undertaken collaboratively and in partnership with all agencies across the borough.

2. Purpose of the Protocol

2.1 The aim of this information sharing protocol is to formally document:

- How the organisations party to this protocol will share information within Children's Services which incorporates a Multi-Agency Safeguarding Hub (MASH) for children and young people aged 0-19 years, which have come to the attention of their organisation.
- The types of information that may be shared and why
- Note the legal framework within which the information is shared
- Set up a framework for information use and sharing that protects the privacy of individuals and provides safeguards for sharing data fairly
- Define the purposes for which partners have agreed to share information
- Describe the roles and structures that will support the exchange of information
- Set out the security procedures necessary to ensure compliance with data protection legislation and any agency specific security requirements
- Describe how this operational arrangement will be monitored and reviewed

2.2 The signatories to this protocol represent the following agencies/bodies:

- Enfield Council
- Enfield Metropolitan Police Service
- Enfield Clinical Commissioning Group
- Barnet, Enfield and Haringey Mental Health Trust
- Enfield Community Services (Health)
- North Middlesex University Hospital NHS Trust
- Royal Free NHS Foundation Trust (including Chase Farm Hospital)

- National Probation Service
- London Community Rehabilitation Company

2.3 It is assumed that each organisation party to this protocol:

- is a registered data controller with the Information Commissioner's Office
- acknowledges its responsibilities under / is compliant with current data protection legislation
- has a complaints procedure that gives individuals recourse to independent investigation in the event of inappropriate sharing of information
- ensures that only anonymised data is used for business planning and research purposes

2.4 The MASH concept for Children's Safeguarding intends to provide the highest level of intelligence and information across the safeguarding partnership to ensure:

- there is effective sharing of intelligence between the agencies within the hub to better co-ordinate risk management processes to ensure that children and young people are properly protected
- safeguarding activity and intervention is timely, proportionate and necessary

Section 10 of the Children Act 2004 created a requirement for children's services to make suitable arrangements for co-operation between the relevant partners in order to improve the wellbeing of children in the authority's area. Statutory guidance for Section 10 of the Act states good information sharing is key to successful collaborative working and arrangements should ensure information is shared for strategic planning purposes and to support effective service delivery.

3. Reasons for sharing information

3.1 Information upon which safeguarding decisions are made in relation to children and young people is held by multiple statutory and non-statutory agencies. Examples of cases across the UK have highlighted deficiencies within safeguarding partnerships in relation to the sharing of information and communication. Some serious case reviews and inquiries have directly attributed the lack of good information sharing and communication to the subsequent death of an individual.

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

In order to deliver the best safeguarding decisions which ensure timely, necessary and proportionate interventions, decision makers need full information concerning an individual and their circumstances to be available to them. Information viewed alone or in silos may not give the full picture or identify the true risk.

3.2 Section 11 of the Children Act (2004) and section 175 of the Education Act (2002) impose a statutory duty upon certain Public Authorities to ensure their functions are discharged 'having regard to the need to safeguard and promote the welfare of children': these authorities include social services, health, police, probation and schools.

3.3 The Children Act (2004) emphasises that the authorities must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area.

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 nineteen or under, or under 25 and having received certain types of social care under Sections 23C to 24D of the Children Act (1989).

3.4 Partners are expected to adopt the statutory guidance issued under the Children Act (2004) *Working Together to Safeguard Children (2015),* and the associated "*Information Sharing: Guidance for practitioners and managers (2015).*

Working Together statutory guidance says:

"Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children. To ensure effective safeguarding arrangements:

- *All organisations should have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and with the LSCB; and*
- *No professional should assume that someone else will pass on information which they think may be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to suffer harm, then they should share the information with local authority children's social care".*

The London Child Protection Procedures, 5th edition (2015) made under the local arrangements further promotes co-operation between relevant partner agencies.

The Data Protection Act 2018, Schedule 1 Part 2 s.18 also provides exemptions to the consent requirements of the data protection law for certain matters of safeguarding for persons under18 and those aged 18 or over and at risk.

3.5 The MASH model was highlighted in the Munro Report into Child Protection as an example of good practice in multi-agency partnership working because of how it improved information sharing between participating agencies.

3.6 The MASH helps deliver three key functions for the safeguarding partnership:

- **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.

- **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.

- **Coordination 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 coordination of harm reduction strategies and interventions

4. Legal basis for sharing and what will be shared

4.1 Legislative powers

Various acts contain expressed or implied powers to share information. The two which are specifically relevant to this protocol and give the statutory framework within which a MASH service operates are:

a) The Children Acts 2004 and 1989
b) The Data Protection Act 2018 which enacts the General Data Protection Regulation 2016 into EU law as the "applied GDPR".

4.2 Legislative compliance

The sharing and disclosure of personal data needs to be done in compliance with existing legislation and that which is most relevant to the operation of a MASH includes:

- The Data Protection Act 2018 which enacts the General Data Protection Regulation 2016 into EU law as the "applied GDPR".
- The Human Rights Act 1998
- The Freedom of Information Act (FOIA) 2000
- The Common Law Duty of Confidence
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Mental Capacity Act 2005
- Criminal Procedures and Investigations Act 1996

Detail on the how this legislation relates to the use and sharing of information is contained in *Appendix A.* In complying with legislation the following guidance and procedures will be followed:

- the Caldicott Principles
- the ICO Code of Practice for Information Sharing
- the London Child Protection Procedures, 5th edition, part B1, chapter 4 'Sharing Information'

4.3 Children Act (2004)

Section 10 of the Children Act (2004) created a requirement for children's services to make suitable arrangements for co-operation between the relevant partners in order to improve the wellbeing of children in the authority's area.

Statutory guidance for Section 10 of the Act states good information sharing is key to successful collaborative working and arrangements under this section should ensure information is shared for strategic planning purposes and to support effective service delivery. It also states these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations.

In response, the London Child Protection Procedures – (5th edition 2015) stipulated that the creation of a MASH is a suitable arrangement to promote the required co-operation between relevant partner agencies.

4.4 First Data Protection Principle: Data must be processed lawful and fair

In order to share information the local authority must have a legal power to do so, as set out below:

The first data protection principle states that data must be processed in a lawful, fair and transparent way.

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 protocol 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, local authorities and relevant health authorities 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.

This legislation supported by the guidance 'Working together to safeguard children', gives the statutory power for agencies to work together and share information where necessary.

Although data protection legislation does not give a power to disclose information, it does state that if not disclosing information would prejudice the prevention/detection of crime and/or the apprehension/prosecution of offenders, personal data, can be disclosed.

Furthermore, under this agreement, if not disclosing information to the MASH would prejudice the reasons listed above, organisations are then exempt from the usual non-disclosure provisions and may provide the information requested / they wish to proactively share without consent. However, this will be decided and recorded on a case-by- case basis.

The sharing of information should be fair and transparent.

Fairness will be based on whether individuals have been told how their information will be used when It is collected and who it may be shared with. Hence fairness requires transparency.

Transparency will be based on whether individuals have been given all the information required under the data protection legislation at the time of collection, and that this data use has been properly assessed and the assessment published according to the regulations.

4.4.1 Duty of Confidence

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that the 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 Child Abuse Investigation Command Standard Operating Procedures) by the MASH Public Protection Desk (MASH PPD). Whilst still applying proportionality and necessity to the decision, the protection of children or other vulnerable persons would clearly fulfil a public interest test

when passing the information to a partner agency whose work with the police would facilitate this aim.

Information held by other agencies that will be 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.

Obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought and documented from and freely given by the data subject.

However, in many cases the aims of the MASH might be prejudiced if agencies were to seek consent. In such cases the disclosing agency **must** consider whether it is possible to disclose personal information without consent. It is possible to disclose personal information without consent if this is in 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 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?

The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject. This should balance the above factors in conjunction with the wishes of the data subject and the wider public interest.

When overriding the duty of confidentiality, the MASH must seek the views of the data-holding organisation that holds the duty of confidentiality and take into account its views in relation to breaching confidentiality. The data-holding organisation may wish to seek legal advice if time permits. All disclosures must be relevant and proportionate to the intended aim of the disclosure.

4.4.2 Fair processing

a) Fairness rests on whether the data subject was deceived or misled as well as whether information was provided about how data will be processed by the signatories to this ISA.

b) Signatories agree to ensure that privacy notices (i.e. Being transparent and providing accessible information to individuals about how you will use their personal data) include details of the information sharing described under this ISA and that they

satisfy the recommendations of law and the Information Commissioner's Office Guidance[1].

c) Signatories agree to consider whether obtaining the consent of the data subjects is appropriate in each case at hand. Consent for MASH checks is obtained verbally.

d) The Data Protection Act 2018 Schedule 1 Part 2 s.18 provides that, disclosures may be lawfully made where obtaining consent would not be possible for a number of reasons and the person is under 18 or over 18 and at risk. Additionally the same section of the act allows disclosures where they are required for either statutory purposes (s.6) or preventing and detecting lawful acts (s.10). Signatories agree that such decisions will be appropriately considered by the MASH Decision Makers, where any decision made to override consent will be proportionate and clearly recorded on the Children's Social Care record.

4.4.3 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.

If possible, consent will be obtained by Children's Services before the case of individuals are brought to the MASH. In these cases, individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why. Consent is obtained verbally and is recorded on the Social Care system.

Details of this and most other non-sensitive information sharing agreements will be published in line with the requirements of the Freedom of Information Act 2000, on the MPS Publication Scheme. This will also allow members of the public to understand how their personal information may be used by the MPS. This is in addition to the ready availability of the Fair Processing Notices mentioned above.

4.4.4 Human Rights Article 8 - The Right for 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 (sub section 1). 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 will be considered on a case by case basis.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

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 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 European Convention on Human Rights 1998, namely the right to life and the right to prohibition of torture or inhuman or degrading treatment. Where sharing of information takes place, there will be consideration of these articles.

- Proportionate
  The amount and type of information shared will only be the minimum necessary to achieve the aim of this agreement. Information is always to be considered in terms of its relevance and proportionality in each set of circumstances, but it must always be remembered that the right to life is paramount and an absolute right.

- 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 NHS bodies and Children's Services also have similar obligations, which are necessary and appropriate in a democratic society.

4.5 **Second Data Protection Principle: Purpose Limitation -** *(data must be collected for specified, explicit and legitimate purposes)*

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.

The MPS 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.

All information will only be used within the MASH for the purposes of safeguarding the vulnerable and reducing harm, which is compatible with the reason it was originally collected.

Signatories agree that information shared under this agreement will be used solely for the purposes identified and that any further processing will be compatible with the identified purposes.

4.6 **Third Data Protection Principle: Data Minimisation -** *(personal data must be adequate, relevant and not excessive)*

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is 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 will be decided on a case-by-case basis and must be relevant to the aims of this agreement.

Examples of data that may be shared include:

- 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
- School and educational information (to include family members where appropriate and relevant)
- Relevant information obtained from GP and Health records
- 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. The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

Signatories agree to consider and document the minimum necessary data set to achieve the purposes of the agreement for each sharing decision **at hand**. This should include consideration of how each piece of information would support the lawful basis and how removal of data might prejudice the purposes for sharing.

4.7 Fourth Data Protection Principle: Accuracy - *(data must be accurate and kept up to date)*

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

All the information supplied will be obtained from signatories' computer systems or paper records and subject to their own organisations reviews, procedures and validation. Where information shared has been found to be inaccurate or out of date, signatories agree to promptly alert sharing partners to allow for review, amendment and incident management.

Whilst there will be regular sharing of information, the data itself will be 'historic' 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.

Signatories agree to take all reasonable steps to ensure information shared and recorded is a statement of fact and the data is accurate and up to date.

4.8 Fifth Data Protection Principle: – Retention (personal data shall be kept for no longer than is necessary)

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. There are specific provisions on the processing of personal data for historical, statistical or scientific purposes.

The data will be kept in accordance with signatories' file retention and destruction policies. 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 historic information for risk assessment purposes. However, once information is no longer needed, it should be destroyed. The principle should be read in light of the "right to be forgotten" under which data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.

For the avoidance of doubt, this principle relates to information shared for the purpose of this Information Sharing Agreement and not as to each organisation's retention policy. If the information shared for the purpose of this agreement is no longer required, then it should be destroyed. If in some cases it may be information which a party would normally hold, then it would fall under that organisation's retention policy.

Please note, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Signatories agree to maintain a records retention schedule in accordance with the necessary legal framework and to de-identify records where lawful and appropriate.

4.9 Sixth Data Protection Principle: – Data Security (personal data shall be processed in a secure manner)

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Signatories agree to transfer information using secure and approved methods such as secure email (nhs.net, egress, office 365 secure email etc.). If secure email is not available, then information will be shared via hand or telephone and contemporaneously recorded in the LCS system.

Signatories agree to ensure that all staff sharing information under this agreement have been provided with a copy and have sufficient training in respect to discharging the agreed procedures.

Signatories agree that appropriate access control and audit procedures will be put in place to prevent unauthorised access to information shared under this agreement.

Signatories agree that information incidents related to information shared under this agreement will be managed according to internal procedures and that relevant updates

and lessons learned will be shared with the signatories.

Signatories agree to ensure that all employees have employment or other relevant contract clauses that include confidentiality and the necessary sanctions for a breach of confidentiality.

4.10 Sharing Protocol

Signatories agree to consider the necessary privacy law framework when making a request or agreeing to share information under this agreement.

Signatories with direct access to source systems such as GP systems, agree not to directly access the records held in those systems without the approval of the Data Controller (please see appendix 1).

Signatories agree to respond within the timescales outlined below to requests and to collaborate with other signatories to support the intention of this agreement in safeguarding the rights and wellbeing of children.

Where possible, the signatory releasing information shall be provided with the rationale for the request for information to support their decision to share information under this agreement.

Dissemination of information shared under this agreement beyond the MASH environment shall be for the purposes identified under Section 5 of those compatible with them and will be completed with proper consideration of privacy law.

5. Enfield's Operational Arrangements

5.1 Strategic Ownership

The Multi Agency Safeguarding Hub (MASH) project was initiated through the Congress of Leaders. It is supported by the GLA and London Councils, and is led by the London Safeguarding Children's Board (LSCB) and Association of London Directors of Children's Services (ALDCS).

MASH underpins the Anti-Violence Partnership strand of the London Crime Reduction Board (LCRB) strategy and addresses Health and Schools and Children's Services prevention, early intervention and safeguarding strategies and duties.

5.2 Governance

Since April 2013, governance of the MASH has transferred to the Quality Assurance Subcommittee of Enfield Safeguarding Children Board.

The Enfield Safeguarding Children Board is responsible for the strategic oversight of the MASH and MASH.

This agreement will be reviewed annually or sooner in response to an incident or as agreed by the signatories.

The signatories agree to meet if required to discuss information sharing under this

agreement and the meetings will include discussion of; lawfulness, proportionality, fairness, incidents, legislation change, incidents, complaints, technical and organisational measures in place to protect the data.

5.3 The MASH - key details

- The MASH comprises a MASH process at its core plus additional agencies (listed in the table below). Through these agencies it will help ensure expertise is joined up to screen and appropriately respond through the co-ordination of targeted single or multi-agency strategies and interventions.

- It will deliver a service to the child and/or family based on the entire partnership knowledge. Information sharing between the agencies will ensure that the necessary, proportionate and most effective intervention is provided.

- It is designed to make information available in one place and to aid communication between partners. By ensuring all partner agencies have the ability to share information, it will help to quickly identify those who are subject to, or likely to be subject to harm. This process will keep individuals safe from harm and assist agencies party to this protocol in discharging their obligations.

- It will help deliver three key functions for the safeguarding partnership:

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

    2. Identification of and reduction in risk to children's wellbeing and welfare:
       Identify children, young people and families who have experienced or are likely to experience harm and ensure partners work together to build resilience and to deliver prevention, early intervention and harm reduction strategies and interventions.

    3. Co-ordination of all safeguarding partners:
       Ensure that the needs of all vulnerable people are identified, signposted to the relevant partner/s and responded to through the co-ordination of targeted single or multi-agency strategies and interventions.

5.4 MASH - Multi-Agency Partnership

Core Co-located MASH partners	Key Virtual MASH Partners
Children's Social Care	Behaviour Support Service (BSS)
Health Safeguarding *(also representing other health services i.e. health visiting, school nurses, FNP)*	CAMHS/SAFE
Independent Domestic Violence Advisor *(via Victim Support)*	Change and Challenge
Police *(via Public Protection Desk)*	CHANNEL / PREVENT
	Cheviots, Joint disability services for children
	Child Development Team (CDT)
	Children's Centres
	Community Safety Unit (CSU)
	COMPASS (Sort It! & Hidden Harm)
	DAZU
	Education Welfare Service
	Educational Psychology Service (EPS)
	ECYPS – community voluntary services (representing e.g. Samafal, Saheli, FECCA and others)
	EN-Able
	Family Nurse Partnership (FNP)
	National Probation Service & CRC (community rehabilitation company)
	PAARs
	Parent Support Unit
	Schools & nurseries
	St Christopher's Young Runaway Project
	Youth Offending

6. Enfield's Local Arrangements

6.1 Obtaining Consent

There are many situations in which a professional can share information legally without obtaining consent from a child or his carer. These are not limited to situations where there is an imminent danger or risk of harm to a child. Frequently, when an assessment of the risk factors affecting a child or family is being undertaken, information will be shared without consent (relying upon statutory powers and duties) when consultation has taken place with a line manager or designated safeguarding professional.

It is good practice for all professionals to obtain consent before sharing information, even when there is no legal requirement. However, consent should not be a barrier to information sharing where there is a safeguarding concern about a child. The MASH will ensure that once a referral is received, issues of consent will be considered on a case by case basis, depending on the level of identified risk and nature of concern
All information received, with or without consent, will be recorded on the Enfield Liquidlogic Children's system (LCS) database, including details of the identified risk of harm. In addition, if a professional shares information without seeking consent, this should be clearly recorded by the professional, including the reasons for not seeking consent.

6.2 Sharing Information when there are Child Protection Concerns

In general, professionals should seek to discuss any concerns with the family and, where possible, seek their agreement to making referrals to children's social care. However, there will be some circumstances where professional should not seek consent when to do so would:

a) Place a child at increased risk of significant harm;
b) Place an adult at increased risk of significant harm;
c) Prejudice the prevention or detection of a serious crime;
d) Lead to unjustified delay in making enquiries about allegations of significant harm.

In some situations there may be a concern that a child may have suffered, or is likely to suffer, significant harm or of causing serious harm to others, but professionals may be unsure whether what has given rise to concern constitutes 'a reasonable cause to believe'. In these situations, the concern must not be ignored.

When in doubt, professionals should always talk to their agency's designated safeguarding children professional for further guidance. Overall, the child's interests must be the overriding consideration in making any decisions whether or not to seek consent.

6.3 The MASH partnership will:

- Share information that is necessary, proportionate and relevant to assist the MASH process and Early Help process (when consent has been gained).
- For referrals that do not reach threshold for statutory intervention, consideration should be given to what information can and should be shared without consent with other agencies for the purpose of promoting and preserving the safety and wellbeing of a child.

6.4 Information entering the MASH specifically from Met POLICE:

Information sharing is vital to safeguarding and promoting the welfare of children and young people. A key factor identified in many serious case reviews (SCRs) has been a failure by practitioners to record information, to share it, to understand its significance and then take appropriate action. For example, when there is a child or unborn child in a family where allegations of domestic abuse are made then Police have the right to share information. The 'Every Child Matters' policy applies to everyone who works in any capacity with children, or providing services to children. This includes professionals such as teachers, social workers, foster carers, hospitals, children's homes, social services and the police, as well as any voluntary groups or charities who work with children.

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.

Police officers based in the MASH as part of the Public Protection Desk (PPD) will review these PACs to see if there is a need to inform Children's Services that the child has come to police attention. They will independently check the Enfield Liquidlogic Children's system (LCS) database to see if there is an open case about the child. Where there is, they will forward the PAC to the MASH for this to be shared with the responsible case worker.

Where there is no open case on the child, the police officers will conduct further research about what other relevant information the MPS has relating to the welfare of the child. They will send the initial PAC and subsequent research via secure email to the MASH for social care oversight and screening by a decision–making qualified social worker (i.e. social work manager or advanced social work practitioner).

6.5 Information entering the MASH from NON-Met Police sources:

Referrals to the MASH by non-met police sources should be related to an identified safeguarding risk for a child. Necessary, proportionate and relevant information should be shared with the MASH to enable the MASH decision maker to clearly ascertain the nature of risk that is being identified for the child.

In contrast to the process for information entering the MASH from the police, the MASH decision maker will also consider if specific information needs to be shared with the PPD Police Sergeant or Police Officer co-located within the MASH where it has been identified that a crime has been committed, but **not** directly related to concerns about child abuse.

This may relate to instances of actual crimes that may not have been reported, or criminal intelligence that may benefit further investigation by police. If it is agreed that the identified information pertains to a crime or relevant criminal intelligence, where appropriate, this will be recorded by the sergeant or police officer for a crime report to be started. A decision will then be taken between the MASH decision maker and PPD officer as to whether any further action can be taken by the MASH or whether the MASH should wait for the conclusion of any necessary police investigation. The decision making around this will be mutually recorded on both police and LCS systems as necessary.

6.6 How the information received in the MASH is processed, irrespective of source:

Upon receiving a new referral, irrespective of source, the MASH will load a new contact record on the LCS, where a MASH decision maker will screen the information received

within twenty-four hours and record the level of identified risk and determine what (if any) other agencies should be approached for relevant information in order to inform a safeguarding decision. These agencies will then be asked to provide relevant information for a MASH investigation, for use in informing a decision about how best to safeguard the child's well-being and what subsequent actions are appropriate to this effect.
This information is required so that a full a picture as possible is known about the child, so that the best and most appropriate assistance can be given to them in the quickest amount of time.

Information gathering by the MASH can also typically include speaking to parents / carers.

Based on an assessment of all the information gathered, the MASH decision maker will then decide what the most suitable course of action will be, which is typically one of the following outcomes:

1. Escalation to children's social care;
2. Referral to Early Help & Prevention services or other agencies;
3. Signposting / information sharing;
4. No further action;

Where relevant, information will then be passed on to the agencies who 'need- to-know' that information in order to appropriately interact with that child and/or their family.

6.7 Sharing information for Early Help & Prevention:

Early Help and prevention is about how different agencies work together to help children, young people and their families, at any point in their lives, to prevent or reduce difficulties. This can often include the need to share confidential information not only between the MASH and Early Help partner agencies, but also between partner agencies outside of the MASH remit.

Early Help provision does not provide a lawful basis for sharing information in and of itself. For the requirement to be met under data protection legislation, explicit consent from the parent/carer of the child or young person whose personal data a professional intends to share, needs to be obtained and clearly recorded.

6.8 Rights of data owner and confidential information:

The MASH is a confidential environment and access to it should only be by those authorised to work within it for the purpose of information sharing in order to assess referrals and contribute to safeguarding decisions.

Information in the MASH must be classed as either confidential or non- confidential. Both types of information will be revealed within the MASH to the MASH Decision Maker in order so they can see the full informed picture upon which to make a decision. Only the data owner, MASH worker leading a MASH investigation (which may include unqualified case workers known as MASH 'care coordinators') and the MASH Decision Maker for a given case should be able to see information provided for the purpose of supporting assessment decisions.

MASH operates a core principle that any organisation revealing confidential and non-confidential information for the purposes of a MASH investigation or safeguarding

consideration within the MASH will always retain the duty of care over the data and remain the data owner.

In practice this means the organisation owning the information, or data owner, has the right to decide not to allow information to leave the MASH after screening or MASH investigation if they believe it to be of a confidential nature and are not prepared to have it shared openly. This decision, which can be discussed with the respective MASH Manager/Decision Maker on a case by case basis, remains at all times with the data owner and must be recorded.

In the case of an unresolved disagreement in relation to information sharing, the designated safeguarding person for the service will be informed where it is felt sharing specific information is pertinent to promote and preserve the safety and wellbeing of a child.

Should information be held back within the MASH at the request of a data owner it must be clearly signposted on any document leaving the MASH in order that operational staff become aware at the earliest opportunity that it exists and who/where they can approach to discuss it further. The information can then be discussed in confidence between the data owner and operational staff on a clear 'need to know' basis.

Please note that information shared by partner agencies is for MASH risk assessment purposes only and is not to be used for any subsequent assessments outside the MASH process and not to be released without the express permission of the data holder.

6.9 Requests for data from MASH records:

Should information be requested from MASH records by way of any judicial process the original data owner must be advised and requested to decide on disclosure or not and manage any specific process required to protect confidential information and its sources. Legal advice should be sought at the earliest opportunity**.**

6.10 Business Continuity:

All partners to this protocol will provide a list of contacts to deal with queries and requests for information under this protocol. The organisations will also nominate persons to act as the contact to ensure continuity in the absence of the original points of contact.

If secure email is not available, then information will be shared via hand or orally, and recorded contemporaneously on LCS.

All information will be recorded centrally but each partner will need to keep local records so that their organisation is aware of how its information is being used.

6.11 Confidentiality and Vetting:

The information to be shared under this protocol is classified as 'RESTRICTED' under the Government Protective Marking System. Vetting is not mandatory to view this grade of information; however staff working within the MASH environment will be vetted to enhanced CRB level. What is required at 'RESTRICTED' level access is that staff viewing shared information will be on a strict 'need-to-know' basis.

Signatories to this protocol agree to seek the permission of the originating agency if they wish to disseminate shared information outside of the MASH environment. Such permission will only be granted where proposed sharing is within the agreed

principles: i.e. for policing purposes, safeguarding and supporting the wellbeing of children

In the event of the data holder wishing to seek advice prior to the release of information when consent has been overridden within the MASH investigation, the designated safeguarding professional for the organisation should be informed by the data holder.

6.12 Compliance:

All signatories to this protocol 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 protocol.

Signatories shall have in place throughout the period of the agreement an Information Security Management Procedure and shall ensure that all relevant employees are made aware of and trained in regards to the Procedure.

Signatories undertake within twenty-four (24) hours, to notify the other partner bodies of any information security breach and/or any breach of the obligations pursuant to data protection legislation and/or the GDPR, together with the steps the partner body who suffers the breach shall take to rectify the breach and to avoid any future such breaches occurring.

6.13 Sanctions:

Any unauthorised release of information or breach of conditions contained within this protocol will be dealt with through the relevant partner's internal disciplinary procedures. Non-compliance and/or breaches of the security arrangements with regards to police information will be reported to the MPS Enfield Borough and reviewed for any risk in the breach. In extreme circumstances, non-compliance with the terms of this protocol may result in the protocol being suspended or terminated.

6.14 Training / Awareness:

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

6.15 Partner's Office and Building Security:

Access to the MASH environment will be controlled by photo access proximity cards and access will be monitored and audited quarterly for all non-permanent Enfield council staff. Access to the Police inner room, housing the Police National Database and VISOR, will be controlled by a coded number lock, known only to Police staff. Members of the public will not have access to the MASH.

6.16 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 via secure, appropriate and approved methods. The sharing of any information must be done via secure email, meaning only email addresses with .pnn, .gcsx, .cjsm, .gsi and nhs.net will be used.

Where a receiving or submitting agency does not have access to a secure e-mail system, documents must only be transferred securely via an alternative encryption service

via EGRESS or USO-FX. This is not an exhaustive list.

6.17 Storage of Information on Partner's System:

The MASH case records will be stored on Enfield Council's relevant IT database, namely LCS. 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.

All Signatories to this protocol 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 MASH information held electronically by partners will be granted on a strict 'need-to-know' basis once it is contained within partners' electronic systems.

6.18 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 in particular is only assessed when needed and stored correctly and securely when not in use.

6.19 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 protocol will be the subject of review by the partner agencies and destroyed in accordance with each agencies code of practice in handling information and with regards to their responsibilities under the Data Protection Act 2018.

Information stored by partners electronically on their systems must be overwritten using an appropriate software utility e.g. Norton Utilities or storage devices destroyed.

6.20 Disposal of Papers

It is not the intention that information will be produced in a hard format. If information is printed off, it is the partner's responsibility to shred the documents using their supplied shredder and follow the Civic Centre's procedure for disposal of confidential waste.

6.21 Review

The arrangements held within this document will be reviewed at yearly intervals or as needed prior to this.

6.22 Freedom of Information Requests

This document is disclosable for the purposes of the Freedom of Information Act 2000. Any requests for information made under the Act that relates to the operation of this protocol should, where applicable, will be dealt with in accordance with the Code of Practice under S.45 Freedom of Information Act 2000. The partner that receives the request will deal with it according to their organisation's procedure. However, the Code also addresses the situation where an organisation may also transfer all or part of a request to another organisation if it relates to information they do not hold.

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.

6.23 Data subject rights

Irrespective of the terms of this Specific Agreement, a data subject may exercise his or her rights under data protection legislation in respect of and against each of the named Parties. For example, if a data subject wishes to delete or amend their records these requests will be dealt with under the provisions of the Data Protection Act 2018.

Appendix A: Summary of Information Sharing Legislation

1. General data protection regulation (GDPR) legislation as enacted by the Data Protection Bill 2018

1.1 Conditions for Processing Personal Data (Article 6 GDPR):

1. The data subject has given consent to the processing for one or more specific purposes.

2. The processing is necessary-
   a. for the performance of a contract to which the data subject is a party, or
   b. in order to take steps at the request of the data subject prior to entering into a contract.

3. The processing is necessary for compliance with a legal obligation to which the controller is subject.

4. The Processing is necessary in order to protect the vital interests of the data subject or of another individual.

5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point 6 above shall not apply to processing carried out by public authorities in the performance of their tasks.

1.2 GDPR Article 9 - Conditions for Processing Special Categories of Personal Data

1.21 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

1.22 Paragraph 1.21 shall not apply if one of the following applies:

a. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

2. The Human Rights Act (1998)

The Human Rights Act (1998) incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be read compatibly with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may be the subject of a legal action under section 7. This is an obligation not to violate Convention Rights and a positive obligation to uphold these rights.

The sharing of information between agencies has the potential to infringe a number of Convention Rights. Whilst Article 3 (Freedom from torture or inhumane or degrading treatment) and Article 1 of Protocol 1 (Protection of Property) may be infringed, the most likely infringement would be to Article 8 (Right to respect for private and family life).

Article 8.1 provides *that "everyone has the right to respect for his private and family life, his home and his correspondence".*

Article 8.2 provides that *"there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others".*

Article 8 ECHR does not provide an absolute right to non-interference with privacy as
Article 8.2 provides a qualification of Article 8 and interference with the Right may be justified if the circumstances of the particular case.

It is always necessary to ensure that there is a legal basis for the action being taken, that it pursues a legitimate aim (as set out in the particular Convention Article) and that it is that the action taken is proportionate and the least intrusive method of achieving that aim. In addition, all Convention Rights must be secured without discrimination on a wide variety of grounds under article 14.

3. The Freedom of Information Act (FOIA) (2000)

The Freedom of Information Act (2000) applies to all public authorities and came into force on 1 January 2005. The Act created new rights of access to information (rights of access to personal information will remain under the Data Protection Act) and revises and strengthens the Public Records Acts 1958 & 1967 by re-enforcing records management standards of practice.

The Lord Chancellor has issued a code of practice on the management of records under FOIA. The principle is that *"any freedom of information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place".* Further information and guidance can be found at the following web site http://www.informationcommissioner.gov.uk

4. The Common Law Duty of Confidence

The Common Law Duty of Confidence requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm.

5. The Caldicott Principles

Both Social Care and NHS organisations that are party to the Protocol are committed to the Caldicott principles when considering whether confidential information should be shared. These Caldicott Principles are:

- Justify the purpose(s) for using personally identifiable information
- Don't use personally identifiable information unless it is absolutely necessary
- Use the minimum necessary personally identifiable information
- Access to personally identifiable information should be on a strict need to know basis
- Everyone must be aware of his or her own responsibilities
- Every member of staff and every organisation party to the protocol must understand and comply with the law (most importantly, the DPA 1998)

6. Computer Misuse Act (1990)

It is illegal to access data without authorisation. This type of activity is known as 'hacking'. There are three offences under this Act:

- Accessing data or programmes held in a computer without authorisation
- Accessing data or programmes held in a computer without authorisation with the intention of committing a further offence, e.g. fraud, blackmail
- Modifying data or programmes held in a computer that you are not authorised to modify
- Accessing data using another person's password is an offence under this Act.

7. Crime and Disorder Act (1998)

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, the probation service, or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act. However, whilst agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information and so responsibility for the disclosure remains with the agency that holds the data. It should be noted that this does not exempt the provider from the requirements of the 2nd principle of the Data Protection Act.

8. Criminal Justice Act (2003)
This Act became law on 20 November 2003 and imposes new risk assessment obligations in relation to violent or sexual offenders. For the first time, some of those obligations fall on the NHS and social care, education, social security and housing bodies. The new obligations relate to Multi-Agency Protection Arrangements (MAPPA) and covers "relevant sexual and violent offenders" including anyone who:

- is subject to notification requirements of Part 2 of the Sexual Offences Act 2003
- has been, or has behaved in a manner that makes him/her liable to be disqualified from working with children
- has been convicted of murder
- has been convicted of one of a number of other offences, including specified sexual offences
- has been convicted of manslaughter, kidnapping, wounding with intent, causing grievous bodily harm, robbery, burglary, affray, or racially or religiously aggravated assault

9. Mental Capacity Act (2005)
Under the Mental Capacity Act, from the age of 16, capacity to consent is assumed, unless there are indications that the person lacks this capacity, in which case a mental capacity assessment is carried out in relation to the particular decision in question and there is a duty to facilitate people's own decision-making where feasible.

If this assessment confirms a lack of capacity, consent may be obtained from a person holding Lasting Power of Attorney (LPA) in respect of the individual's health and wellbeing, or a person action their behalf under the Court of Protection. An individual may have more than one LPA appointed to make decisions regarding their welfare and / or financial affairs.

The relevant LPA should be consulted depending on the information sharing required. If no such person exists, staff will make a 'best interest' decision on disclosure, involving family and other interested parties where possible.

10. Criminal Procedures and Investigations Act (1996)
This Act requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

11. ICO Framework Code of Practice for Information Sharing
This framework code of practice contains practical advice that will help all those involved in information sharing to develop the knowledge and confidence to make appropriate decisions about sharing personal information. This framework code of practice aims to help make sure that the benefits of information sharing are delivered, while maintaining public trust and respecting personal privacy.

12. Regulation of Investigatory Powers Act (RIPA) (2000)
The Regulation of Investigatory Powers Act 2000 primarily deals with the acquisition and disclosure of information relating to the interception of communications, the carrying out of surveillance and the use of covert human intelligence. It is unlikely that this Act will have any implications on the sharing of personal information.

13. Protection from Harassment Act (PHA) (1997)
This Act is specific to the information sharing protocol agreement between Enfield Council's Housing department and the Metropolitan Police Service. It relates to action amounting to harassment or putting people in fear of violence, as defined by the Act, in respect of a person residing in or visiting at an address, in which the housing authority has a landlord's interest or where the action was aimed at premises run or peopled by the housing authority.

14. Housing Act (1985), Housing Act (1996) and Anti-social behaviour, Crime and Policing Act 2014
These Acts are specific to the information sharing protocol agreed between Enfield's Housing Department and the Metropolitan Police Service and other agencies (such as Registered Social Landlords). In particular, the ASBCP 2014 reorganises and enhances the powers available to landlords to deal with anti-social behaviour.

15. Local Government Act (LGA) (2000)
The LGA 2000, Section 2, permits many types of data sharing partnerships between local authorities and others where the proposed data sharing will achieve the promotion or improvement of the economic, social and environmental well-being of their area.

16. Other Legislation
Further Acts may apply, e.g. **Prevention of Terrorism Act (2002), Health and Social Care Act (2001), Environmental Information Regulations, Criminal Justice Act (2003).** Further information about these or any other relevant legislation can be found at the HMSO website http://www.hmso.gov.uk/