INFORMATION SHARING PROTOCOL
for
ENFIELD’S SINGLE POINT OF ENTRY (SPOE)

Incorporating a Multi-Agency Safeguarding Hub (MASH)
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 Enfield’s Single Point of Entry (SPOE) system which incorporates a Multi-Agency Safeguarding Hub (MASH) about children and young people, aged 0 -19 years who have come to the attention of their organisation for failing at least one of the five Every Child Matters (ECM) outcomes

- the types of information that may be shared and why

2.2 This protocol sits below the Enfield Safeguarding Children Board’s information sharing protocol. It does not cover other sharing between the signatory agencies that takes place outside of the SPOE - these are covered (where appropriate) by separate protocols.

It has been developed specifically for the operation of Enfield’s (SPOE) to:

- 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 the Data Protection Act and any agency specific security requirements
- Describe how this operational arrangement will be monitored and reviewed

2.3 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

2.4 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 the Data Protection Act (DPA) 1998
• 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

2.5 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 many statutory and non-statutory agencies. Many sad 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.


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”.


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.

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 relevant to this protocol and give the statutory framework within which a MASH operates are

a) The Children Act 2004 and

4.2 Legislative compliance
ESCB SPOE & MASH Information Sharing Protocol
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:

- Data Protection Act 1998
- 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 Data Protection Act (1998) (DPA)

The 8 principles of the DPA are listed below and form the structure for describing the framework for how information will be shared and used.

4.4.1 First Principle: Data must be processed lawfully and fairly.

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

The sharing of information should be lawful and fair.

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.

**What does this mean?**

Consent is not necessarily the only condition for sharing information through MASH. This is especially the case if seeking consent will have serious consequences on the physical or mental wellbeing of a child or another individual.

The decision not to seek consent in advance of information sharing must be considered on a case by case basis using professional judgement and reasons for any such decision must be recorded.

**Duty of Confidence**

When overriding the duty of confidentiality the MASH must seek the views of the organisation which 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. All disclosures must be relevant and proportionate to the intended aim of the disclosure.

This is particularly relevant to information obtained from the police. Before any disclosure is made of information from the police checks must be made to ensure that disclosure will not affect any ongoing investigation.

**Fair Processing**

It is a requirement of the Data Protection Act 1998 that all organisations that process personal data should have a ‘Fair Processing Notice which will inform individuals about how their personal data will be used by that organisation. This notice will cover:

1. The identity of the data controller
2. If the data controller has nominated a representative for the purposes of the Act, the identity of that representative
3. The purpose or purposes for which the data are intended to be processed.
4. Any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

**Legitimate Expectation**

Details of this information sharing protocol will be published in line with the requirements of the Freedom of Information Act 2000 to allow members of the public to understand how their
personal information may be used by the partnership. This is in addition to the ready availability of the Fair Processing Notices mentioned above.

- **Data Protection Act 1998, Schedule 2**

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

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

Where the consent of the individual is received, Condition 1 (data subject has given consent to the processing of their data) will apply.

- **Data Protection Act 1998, Schedule 3**

If the information is “sensitive” (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3 as well as a Schedule 2 condition.

Schedule 3 is satisfied in the case of this protocol by condition 7, “the processing is necessary for the exercise of any functions conferred on any person by or under an enactment” (i.e. as mentioned above, Children Act (2004)). Where this condition is not satisfied for the disclosure that is being considered then other conditions may be available.

**Section 29 Exemption – Prevention or Detection of Crime**

Under Section 29 of the Data Protection Act 1998 provision is made for disclosure of information where it is necessary for the purpose of a criminal investigation and or prosecution. In other words if not disclosing information to the Police or other law enforcement agencies would prejudice the purposes referred to in the Section 29, organisations are then exempt from the usual non-disclosure provisions (with the exception of meeting a schedule 2 and 3 condition) and may provide the information requested / they wish to proactively share. This will be decided though on a case-by-case basis.

Section 29 of the Data Protection Act 1998, allows agencies to share information without the requirement of complying with the fair processing conditions (i.e. telling individuals how their data will be processed/shared) if by doing so it would be likely to prejudice the purposes of the prevention or detection of crime and/or the apprehension and prosecution of offenders. This decision will be taken on a case-by-case basis.

Recordings of the reasons behind the decision must be kept where consent is not given.

- **The Right for respect for private and family life, home and correspondence - Human Rights - Article 8**

“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 information with the Enfield MASH could contravene Article 8.

However, the rights set out in article 8 are qualified so a public authority may interfere in private and family life as set out in the article.

In order to demonstrate that any interference with private and family life complies with article 8, it is essential that record keeping demonstrates that this protocol has been followed and that at least one of the reasons permitting interference applies.

This protocol 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 protocol. The sharing of information under this protocol 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.

- **Proportionate** – the amount and type of information shared will only be the minimum necessary to achieve the aim of this protocol. 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** – each agency which is a signatory to this protocol, is 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.

---

**Caldicott Guardian**

As a result of the 1997 report of the Review of Patient-Identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report), each NHS organisation has appointed a “Guardian” of person-based clinical information to oversee the arrangements for the use and sharing of clinical information. Subsequently the requirement to appoint Caldicott Guardians was extended into Councils with Social Care Responsibilities.

Key recommendation of the Caldicott Committee was that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the principles developed in the Caldicott Report.

Principle 1 – Justify the purpose(s) for using confidential information
Principle 2 – Only use it when absolutely necessary
Principle 3 – Use the minimum that is required
Principle 4 – Access should be on a strict need-to-know basis
Principle 5 – Everyone must understand his or her responsibilities
Principle 6 – Understand and comply with the law

The Caldicott Guardians for Barnet Enfield & Haringey Mental Health Trust and Enfield Council have been consulted and have signed up to this protocol and will ensure that Enfield’s MASH operates within Caldicott guidelines.
4.4.2 Second Principle: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 
All data that is to be shared is obtained for the purposes of identifying and assessing risks to children and young people. The data is only shared with agencies that are partners with the police in achieving that aim and improving the well-being of children. 
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.

4.4.3 Third Principle: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Any information that is shared within the MASH Hub will be decided on a case-by-case basis and must be relevant to the aims of this protocol. 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)
- GP and health records (to include family members where appropriate and relevant)
- Relevant Anti-Social Behaviour (ASB) data (including but exclusive to noise disturbance)
- 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.
- Relevant information about offenders known to the London Probation Trust

The list above is not exhaustive and 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.

4.4.4 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 each organisation’s reviews, procedures and validation.
Any perceived inaccuracies should be reported to the contact at that agency for verification and any necessary action.

4.4.5 Fifth Principle: Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.
The data will be kept in accordance with signatories’ file destruction policy. It is acknowledged that there is a need to retain data for varying lengths of time depending on the purpose and
also in recognition of the importance of historical information for risk assessment purposes. However, once information is no longer needed, it should be destroyed.

4.4.6 Sixth Principle: Personal data shall be processed in accordance with the rights of data subjects under this Act.
Partners to this arrangement will respond to any notices from the Information Commissioner’s Office that imposes requirements to cease or change the way in which data is processed. Partners will comply with subject access requests in compliance with the relevant legislation.

4.4.7 Seventh Principle: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Measures to satisfy the Seventh Principle are detailed in the HMG Baseline Security Standard document - prepared as part of the development of this protocol and included in Section Four of the purpose specific protocol, “Description of Arrangements including security matters”

4.4.8 Eighth Principle: Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.
The information is not intended for transfer outside the European Economic Area. Any decision to share the information outside this area would be a matter for the partner agency as long as it is shared within the agreed principles: i.e. for policing purposes, which includes safeguarding children. Legal advice may be necessary in these cases.

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.

The London framework incorporates emerging innovative practice from other boroughs and from Devon, which has been independently evaluated as providing better decision making and outcomes for children. The Munro review on Child Protection (10 May 2011) cited Devon MASH as good practice.

5.2 Governance
Since April 2013, governance of the SPOE 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 SPOE and MASH

5.3 The SPOE - key details

- The SPOE comprises a MASH at its core plus additional agencies (listed in the table below). Through these agencies it will help ensure expertise is joined up to plan for and 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 statutory partners have the ability to share information, it will help to quickly identify those who are subject to, or likely to be subject to harm which 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.

5.6 SPOE Membership as at February 2016

<table>
<thead>
<tr>
<th>Core MASH partners - Permanent &amp; Full time / Daily Presence</th>
<th>Wider SPOE Partners with essential &amp; weekly presence</th>
<th>Virtual Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children’s Social Care</td>
<td>Education Welfare</td>
<td>Cheviots, Joint disability services for children</td>
</tr>
<tr>
<td>Health Safeguarding (also representing other health services i.e. health visiting, school nurses, FNP)</td>
<td>Change and Challenge</td>
<td>Gangs Partnership Group (GPG)</td>
</tr>
<tr>
<td>Police</td>
<td>Youth and Family Support</td>
<td>Family Nurse</td>
</tr>
</tbody>
</table>
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. Consent should not be a barrier however to sharing information where there is a concern about a child. The SPOE will ensure that once the referral is received that issues of consent will be considered on a case by case basis.

All information received, with or without consent, will be recorded on the Enfield children's integrated children's database, including details of the risk of harm. In addition, if a professional shares information without seeking consent, this should be clearly recorded, including the reasons for not seeking consent.

6.2 Sharing Information when there are Child Protection Concerns
While, 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, there will be some circumstances where professional should not seek consent e.g. where to do so would:

Place a child at increased risk of significant harm;
Place an adult at risk of serious harm;
Prejudice the prevention or detection of a serious crime;
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.

Professionals should always talk to their agency's designated safeguarding children professional and, if necessary and where they have one, a Caldicott Guardian - who will have expertise in information sharing issues, though not related to child protection. The child's interests must be the overriding consideration in making any decisions whether or not to seek consent.

6.3 The multi-agency partnership will:

- Share information that is necessary, proportionate and relevant to assist the MASH process
- Share information that is necessary, proportionate and relevant to all referrals and collectively decide whether a single agency or a multi-agency response is required. 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.
- If multi-agency support is needed, the SPOE partnership will agree a Lead Agency who is responsible for convening a meeting for the relevant agencies involved together with the family (Team Around the Family/ TAF).
- Each agency will complete checks within their own organisations and bring any relevant information to the SPOE meeting
- The initial TAF meeting will discuss the referral and plan subsequent action and agree the lead professional to implement any plans

6.4 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.
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.

6.5 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

6.6 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.

6.7 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.

6.8 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.

6.9 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. Access to the inner room, housing the Police National Database and VISOR, will be controlled by a coded number lock, known only to Police staff.

6.10 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.

6.11 Storage of Information on Partner’s System
The MASH case records will be stored on Enfield Council’s relevant IT database. 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.
6.12 Storage of Papers
It is not the intention of this protocol that information will be produced in a hard format. Access to printed documents must be limited only to those with a valid ‘need to know’ that information. The MASH will operate a clear desk policy where all partners are responsible for only assessing information when needed and storing securely when not in use. Lockers and lockable under desk storage will be supplied for this purpose.

6.13 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.

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

6.14 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 the supplied shredder and follow the Civic Centre’s procedure for disposal of confidential waste.

6.15 Review
The arrangements held within this document will be reviewed at yearly intervals.

6.16 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.

Appendix A: Summary of Information Sharing Legislation

1. Data Protection Act (1998)
The Data Protection Act (1998) governs the processing of information about living individuals. The Act does not apply to personal data relating to the deceased. Any agency processing
personal data is a ‘data controller’ registered with the Office of the Information Commissioner and must comply with the 8 principles of the Act.

The Act gives seven rights to individuals in respect of their own personal data:

- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the Act)
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

The 8 Principles of the Act are:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Personal data shall be processed fairly and lawfully and shall not be processed unless at least one of the conditions in Schedule 2 is met and, for ‘sensitive personal data’, at least one of the conditions in Schedule 3 is also met.</td>
</tr>
<tr>
<td>2.</td>
<td>Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.</td>
</tr>
<tr>
<td>3.</td>
<td>Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.</td>
</tr>
<tr>
<td>4.</td>
<td>Personal data shall be accurate and, where necessary, kept up to date.</td>
</tr>
<tr>
<td>5.</td>
<td>Personal data shall not be kept for longer than is necessary for that purpose/purposes</td>
</tr>
<tr>
<td>6.</td>
<td>Personal data shall be processed in accordance with the rights of the data subject under this Act.</td>
</tr>
<tr>
<td>7.</td>
<td>Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.</td>
</tr>
<tr>
<td>8.</td>
<td>Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.</td>
</tr>
</tbody>
</table>

Schedule 2 and Schedule 3 conditions:

Conditions for processing personal data are that one condition in Schedule 2 should be met.

Conditions for processing sensitive personal data are that one condition in Schedule 2 and one condition in Schedule 3 should be met.

<table>
<thead>
<tr>
<th>Schedule 2: Personal Data</th>
<th>Schedule 3: Sensitive Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Subject has given consent, or</td>
<td>The Data Subject has given explicit consent, or</td>
</tr>
<tr>
<td>The processing is necessary for:</td>
<td>The processing is necessary for:</td>
</tr>
<tr>
<td>- A contract</td>
<td>- Employment related purposes</td>
</tr>
<tr>
<td>- Legal obligation</td>
<td>- The purpose of, or in connection, with legal proceedings</td>
</tr>
<tr>
<td>- Protection of the vital interests of the</td>
<td></td>
</tr>
</tbody>
</table>
### Data Subject
- Public function
- In the public interest
- A statutory obligation
- Legitimate interests of the Data Controller

### Protection of vital interest of the individual (where consent cannot be obtained)
- Made public by the data subject
- Substantial public interest
- Prevention or detection of an unlawful act
- Legitimate interests of a non-profit making organisation
- Medical purposes

### 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.


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](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)

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.

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.
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

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 acting 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.

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.

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.
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.

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.

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/