

CALDERDALE MULTI-AGENCY SCREENING TEAM (MAST) Purpose Specific Information Sharing Arrangement

Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes
Title	A purpose specific information sharing agreement documenting sharing within Calderdale MAST
Version	4
Summary	An agreement to formalise information sharing arrangements within Calderdale MAST, between Calderdale Children's Services, Calderdale District Police, and Locala/Calderdale and Huddersfield NHS Foundation Trust for the purpose of identifying and assessing risks to children's wellbeing and welfare in the Borough.
Author	Gill Poyser-Young/Laura Knights
Date Issued	July 2015
Review Date	April 2020
Further Review	March 2019
Further Review	Only if significant changes are required

This agreement is to be used in conjunction with the Inter Agency Information Sharing Protocol and complies with all the guidance therein

Sharing of Information within the Calderdale Multi Agency Screening Team (MAST) to assist in identifying and assessing risks to children's wellbeing and welfare in the borough

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners annually.

The day to day management responsibility for MAST lies with the MAST Team Manager and MAST Service Manager. Escalation to partner agencies will take place when required.

Contents

1	Glossary of Terms.....	4
2	Specific purpose(s) for which the information sharing is required.....	5
3	Status of information shared	Error! Bookmark not defined.
4	Purpose.....	9
5	Legal basis for sharing and what specifically will be shared	10
5.1	Legislative Powers.....	10
5.2	Legislative compliance	10
6	Types of information items shared	12
7	Safekeeping and storage of information.....	12
8	Information transfer method.....	12
9	Incidents.....	13
10	Retention and disposal of information	14
11	Staff training.....	14
	Appendix 1 – Laws enabling and governing the sharing of personal data.....	15
	Appendix 2 – Data protection principles and the MAST/MASH	23
	Appendix 3 – Checklists for sharing information under the Data Protection Act 1998.....	27
	Appendix 5 Parties to this agreement	30
12	Storing your data.....	34

1 Glossary of Terms

‘Agencies’, ‘Partners’, ‘Partner/Member Organisations’:- Relates to the organisations specified above which detail the organisations that are signatories to this Information Sharing Agreement.

‘Information’:- Within this Information Sharing Agreement information could include personal and/or sensitive personal data. (Personal data includes name, address, dates of birth. Sensitive data includes racial or ethnic origin, religious beliefs, sexual orientation, physical or mental health or condition, alleged offences.)

‘Anonymised Information’:- Information from which no individual can be identified.

‘Explicit Consent’:- This means articulated agreement and relates to a clear and voluntary indication of preference of choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

‘Implied Consent’:- This means agreement that has been signalled by the behaviour of an individual with whom a discussion has been held about the issues and therefore understands the implications of the disclosure of information.

‘Data Transfer’:- The disclosure of information from one or more organisations to another organisation, which could be routine data sharing where the same data sets are shared between the same organisations for an established purpose; or a ‘one off’ decision to share data for a range or purposes.

‘Data Subject Access Request’:- Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records, by writing to the person or organisation they believe holds it.

‘Data Controller’/‘Data Owner’:- A person or organisation who (either alone or jointly) determines the purposes for which and manner in which any personal data is to be processed.

2 Specific purpose(s) for which the information sharing is required

To enable the Multi-Agency Screening Team (MAST) agencies to share information in a secure environment in relation to identifying and assessing risks to children's wellbeing and welfare, in order to safeguard and protect vulnerable children and young people within the Calderdale District.

The vision is to deliver a commitment to ensure safeguarding standards for the children and young people of Calderdale are robust. The MAST will assist partners in assessing risk and making judgements in relation to referrals and ensure suitable pathways are developed so children and families receive the right level of intervention at the right time.

The MAST will deliver a multi-agency response where professionals or members of the public have expressed concern in relation to a child or young person. It will encourage professional curiosity and challenge agencies to jointly contribute to the assessment of risk.

Partner agencies within the MAST will gather information from all their own agency systems and use this information to better inform their decision making in relation to the type of service the child and / or young person should be offered, on any child or young person who are identified on the Continuum of Need at levels 1-5.

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

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

"Children" in terms of the scope of this Act means all children and young people up to the age of 18.

Partners are expected to adopt the statutory guidance issued under the Children Act (2004) Working Together to Safeguard Children (2018), and the associated "Information Sharing: Guidance for practitioners and managers (2018).

Information sharing statutory guidance 2018 says:

'Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.'

The West Yorkshire Consortium Child Protection Procedures 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 under 18 and those aged 18 or over and at risk.

The Information Governance Review undertaken by Dame Fiona Caldicott in March 2013 states 'the overarching aim has been to ensure that there is an appropriate balance between the protection of the patient or user's information, and the use and sharing of such information to improve care.

The evidence received during the Review resulted in an additional Caldicott Principle:

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality.

The Government has accepted the recommendations of the Caldicott Review, and notes 'This new approach will need to be clear that the public interest may justify sharing information about children and other family members where there are safeguarding concerns.'

Information upon which safeguarding decisions in relation to children and young people are made is held by numerous statutory and non-statutory agencies. Many 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 (such as the Laming, Bichard and Baby P inquiries) have directly attributed the lack of good information sharing and communication to the subsequent death of an individual.

In order to deliver the best safeguarding decisions which ensure timely, necessary and proportionate interventions, decision makers need the full information picture 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.

This has been evidenced/recommendation in numerous serious reviews both locally and nationally.

As such all the information from various agencies needs to be available and accessible in one place. A Multi Agency Safeguarding Team (MAST) helps ensure this and aids communication between all safeguarding partners. By ensuring all statutory partners have the ability, confidence and trust to share information, those who are subject to, or likely to be subject to, harm can be identified in a timely manner, which will keep individuals safe from harm and assist signatories to this agreement in discharging their obligations under the Act.

The MAST 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.
- **Identification and harm reduction to others**
Identify others who are likely to experience harm and ensure partners work together to act and respond appropriately.

- **Co-ordination of all safeguarding partners**
Ensure that the needs of all vulnerable children and young people are identified and signposted to the relevant partner/s for the delivery and co-ordination of interventions and services.

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

The aim of this information sharing agreement is to formally document how, through the MAST set-up, the signatories to this agreement will share information about children who have come to the attention of their organisation who are identified as being on the Continuum of Need.

This agreement does not cover other information sharing arrangements between the signatory agencies that takes place outside of the MAST - these will be covered (where appropriate) by separate information sharing agreements.

3 Status of information shared

Each member organisation should have Fair Processing Notices in place, as it is a requirement of the Data Protection Act 2018 that all organisations that process personal data should have Fair Processing Notices which will inform individuals about how their personal data will be used by that organisation.

Practitioner and MAST requirements:

There are different routes for sharing information between Social Care, Police, Health, Early Intervention and any other agency (all agencies based in the MAST). Decision making/action and signposting to the appropriate services after referral is determined by the Continuum of Need levels 1-5.

Practitioners **must** have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). A referral to MAST is in itself sharing of information. Nevertheless, practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children (Working Together to Safeguard Children, 2018)

At all levels of the continuum of need all practitioners should aim to gain consent to share information, but should be mindful of situations where to do so would place a child at increased risk of harm.

Information may be shared without consent if a practitioner has reason to believe that there is good reason to do so, that the sharing of information will help to determine whether there are any safeguarding risks or enhance the safeguarding of a child in a timely manner.

When decisions are made to share or withhold information, practitioners should record who has been given the information and why (Working Together to Safeguard Children, 2018).

Practitioners must understand their obligations under data protection principles.

Consent must always be the primary option. ALL reasons for dispensing with consent must be **explicitly** recorded on the referral itself and contact/referral page in CASS by the Practice Manager or Team Manager.

MAST Referrals:

Referral to the MAST itself for a safeguarding concern with or without consent is likely always to be in accordance with:

- **“GDPR Legitimate Interest”**: “the sharing of information will enhance the safeguarding of a child in a timely manner”, As well as:
- **“GDPR Public task”**. Particularly, when one considers the MAST is an operational team with duties fulfilling requirements of The Children Act 2004. (Relevant partner agencies - which include the police, children’s services authorities, NHS bodies and others must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children.)

Nevertheless, once referral and screening assessment has taken place **additional** information would need to be evidenced **to continue** information sharing without consent.

Therefore:

- In ALL cases Consent must always be the primary option, **UNLESS** superseded by other GDPR objectives.
- ALL reasons for dispensing with consent must be **explicitly** recorded on the referral itself and contact/referral page in CASS by the Practice Manager or Team Manager.

By way of guidance, the rationale for dispensing with consent must comply with one (or more) of the below GDPR basis:

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone’s life.

For example:

If seeking consent would place a person (the individual, family member, yourself or a third party) at increased risk of significant harm if a child, or serious harm if an adult For example, there was a suspicion that the adult might flee with the child

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

For example:

- If seeking consent would prejudice the prevention, detection or prosecution of a crime . eg Cases of Honour Based Violence, or Forced Marriage
- Attempts to seek consent would lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult: *Information Sharing: Guidance for Practitioners and Managers, (2018) HM Government*

- That the sharing of information will enhance the safeguarding of a child in a timely manner (Working Together to Safeguard Children, 2018).
- To prevent delay if **all reasonable attempts** have been made to seek consent. This must be recorded clearly and include the reasons for dispensing with the consent. This should be done by the Practice Manager or Team Manager of the MAST.

Following the MAST referral and screening process:

The documented rationale for dispensing with consent will inform to what extent partnership information can be further shared.

Sharing of information without consent requires a continuous assessment. The rationale for dispensing with consent may change or be negated over time.

Police

West Yorkshire Police has a dedicated officer within the MAST who has the responsibility to share information with the partner agencies within the MAST.

Purpose

Information sharing enables early intervention and preventative work to safeguard and promote welfare and for wider public protection. The public need to be confident that their personal information is kept safe and secure. All members of the Police service are responsible for ensuring that we share information appropriately as part of our day-to-day practice and do so confidently, proportionately and lawfully.

Health

Locala provides health practitioner representation in MAST to be the conduit for health information from partner health agencies in Calderdale, including GP practices. Only appropriate and relevant health information will be shared in response to the concerns raised.

Health information from partner health internal systems will be shared in accordance with consent to share other agency information via specific information sharing agreements between Locala and other health partner organisations in Calderdale i.e. Calderdale and Huddersfield NHS Trust and South West Yorkshire Partnership NHS Foundation Trust. NB This information sharing agreement does not apply to CAMHS Tier 2 service. The consent to share health information for individual GP practices will be co-ordinated by the Designated Nurse Safeguarding Children in Calderdale CCG on an opt-in basis (See Appendix 4 for letter to GPs re information sharing consent).

The GP consent relates to GP practices only in Calderdale in relation to the child/children, parent(s) and significant other relevant adults involved in the child's life. GP practices who do not use SystemOne for health records will need to be contacted directly by the health practitioner in MAST to obtain relevant health information. Consent will also need to be sought from those GP practices that have not given their consent to the information sharing agreement.

Health information relating to adults or children who are not registered with a GP practice in Calderdale will require explicit consent to be sought from the data controller in the GP practice where they are registered to discuss how relevant information will be shared. There are three possible options:

- MAST health practitioner given explicit consent by the GP practice to access the health records and share relevant information
- MAST health practitioner given relevant health information verbally over the telephone with consent to share
- Consent not given and the GP practice will share information directly into the strategy meeting

Child Sexual Exploitation (CSE)

Information sharing for young people in relation to CSE is also covered by the health interagency information sharing agreements.

Health practitioners in MAST will also ensure that relevant health information (with the exception of sexual health service information as this is a closed system) is available to the weekly CSE multi-agency operational meeting. The health information will be relayed into the CSE operational meeting via a health representative from CAMHS, Locala safeguarding team, CHFT safeguarding team or CHFT Children Looked After team.

Only relevant health information relating to young people on the Calderdale CSE MATRIX, or those on the agenda to be discussed, at the meeting will be shared.

Whenever a health record is accessed by the MAST health practitioner an entry will be made noting that the health record had been accessed for the purposes of MAST.

3 Legal basis for sharing and what specifically will be shared

3.1 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 MAST 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”.

3.2 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 MAST 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
- The Children Act 1989 & 2004
- Working Together to safeguard Children 2015/18
- The Care Act 2017
- Children (Leaving Care) Act 2000
- Crime and Disorder Act 1998
- Criminal Justice Act 2003

- Mental Capacity Act 2005
- Management of Police Information (MOP)
- National Health Service Act 2006
- Access to Health Records 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Criminal Procedures and Investigations Act 1996

Detail on the how this legislation relates to the use and sharing of information is contained in Appendix .

- In complying with legislation the following guidance and procedures will be followed:
- the Caldicott Principles
- the ICO Code of Practice for Information Sharing
- the West Yorkshire Consortium Child Protection Procedures, 'Sharing Information'

All agencies are subject to a variety of legal, statutory and other guidance in relation to the sharing of person- identifiable or anonymised information.

Further detail about key legislation and guidance is contained in the Inter-Agency Information Sharing Protocol.

Further information about how the MAST relates to Data Protection Principles is shown at Appendix 1.

The Calderdale Child Protection Procedures should also be viewed as useful guidance in this area [www.http:calderdale-scb.org.uk](http://calderdale-scb.org.uk)

4 Types of information items shared

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

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

Only relevant information will be shared on a case by case basis where an organisation has a need to know about the information.

Caldicott Principles must be applied:

1. Justify the purpose.
2. Don't use personal confidential data unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

5 Safekeeping and storage of information

MAST is a confidential 'fire walled' environment and access to it should only be by those professionals authorised to work within it for the purpose of information sharing in order to assess referrals and make decisions.

Staff co-located in an environment conducive to information sharing sited in Calderdale, West Yorkshire. The MAST will have with access to IT and telephone systems and can operate in an environment conducive to information sharing in a secure, confidential environment. Each agency will continue to use IT equipment linked to their own agency, and then share information both on a face to face basis and electronically (via secure email). There will be no public access to this area.

The contact/referrals electronic case records will be stored on Calderdale Metropolitan District Council's electronic system, Calderdale Assessment Safeguarding System (CASS), only the professionals working within the MAST will have access to the MAST case records. However other agencies may be passed information from the MAST case record if approved by the original data owner where appropriate for further interaction with a child, which may also be stored electronically.

All information shared will be recorded under the contact/referral or separate meeting minutes i.e. threshold meeting/strategy meeting. Minutes of relevant meetings will be provided to health and police and any other relevant MAST or partner agencies.

6 Information transfer method

All parties to this agreement are responsible for ensuring that appropriate security and confidentiality procedures are in place to protect the transfer and use of the shared, person identifiable information. MAST has its own e-mail account which is secure.

Information entering the MAST from non-police sources:

Information about a child where there are concerns about their welfare will be received by the MAST. A check will be undertaken to see if there is an open case, and if so, forward that information on to the relevant team. Where there is not an open case, the MAST will create a new case record on CASS and pass the information through to the contact/referral process where the MAST and the partner agencies will review the information and determine whether the thresholds are met under the Continuum of Need levels 1-5.

7 Incidents

Any incidents or complaints occurring as a result of this agreement should be reported to the signatories of all affected organisations. They will then pass on the information in accordance with incident reporting procedures within their own organisation if appropriate. Organisations will agree to share information in order to help investigate any such incidents. All complaints will be dealt with under Calderdale Council Complaints Section and the responsible officer will be the Social Care MAST Service Manager who will delegate the complaint where appropriate.

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

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

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

8 Retention and disposal of information

Retention Period For Information	
Disposal Method For Electronic Information	<p>Once information contained within emails is transferred to partner's electronic systems, the emails will be deleted.</p> <p>Information will be held in electronic systems until the information is no longer required. Information provided as part of this agreement will be the subject of review by the partner agencies. Information will be destroyed in accordance with each agencies code of practice in handling information and with regards to their responsibilities under the Data Protection Act.</p>
Disposal Method For Paper Information	<p>It is not the intention of this agreement that information will be produced in a hard format. If information is printed, it will be the partners' responsibility to dispose of the information in an appropriate secure manner (ie shredding, through a 'RESTRICTED' waste system) once it is no longer needed.</p>

9 Staff training

All staff members working within the MAST should be trained and be familiar in all aspects of safe data transfer, and in the operation of the MAST and the legal background for information sharing of personal and sensitive information.

Appendix 1 – Laws enabling and governing the sharing of personal data

1. General Data Protection Regulations (GDPR) legislation as enacted by the Data Protection Act 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 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. Data Protection Act 2018 (DPA 2018)

Schedule 2, Part 1(2) - where disclosure is required for the prevention or detection of crime or the apprehension or prosecution of offenders.

- Where a data controller is obliged by or under any enactment to make personal data available to the public.
- Where the disclosure is required by or under enactment, by any rule of law or by the order of a Court.
- Where the disclosure is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) or for the purpose of obtaining legal advice or establishing, exercising or defending legal rights.

3. Children's Act 1989

Section 17 - general duty of local authorities to safeguard and promote the welfare of children within their area who are in need, and so far as is consistent with that duty, to promote the upbringing of such children by their families.

Section 47 - where a local authority is informed that a child who lives, or is found, in their area is the subject of an emergency protection order or is in police protection or there is reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm, there is a duty to investigate.

4. Children's Act 2004

Section 10 - promote co-operation to improve wellbeing.

Section 11 - arrangements to safeguard and promote welfare.

Section 12 - requirement on children's services authorities in England to establish and operate databases containing basic information about every child in England. The current database is known as ContactPoint.

5. Working Together to safeguard Children 2018

This guidance covers:

- The legislative requirements and expectations on individual services to safeguard and promote the welfare of children;

6. Children (Leaving Care) Act 2000

Section 24C(1) - where it appears to a local authority that a person with whom they are under a duty to keep in touch under section 23B, 23C or 24; or whom they have been advising and befriending under section 24A; or to whom they have been giving assistance under section 24B, proposes to live, or is living, in the area of another local authority, they must inform that other authority.

Section 24C(2) - where a child who is accommodated by a voluntary organisation or in a private children's home, by any Health Authority, Special Health Authority, Primary Care Trust or local education authority or in any care home or independent hospital or any accommodation provided by a National Health Service trust, ceases to be so accommodated, after reaching the age of sixteen, the organisation, authority or (as the case may be) person carrying on the home shall inform the local authority within whose area the child proposes to live.

7. Crime and Disorder Act 1998

Section 17 - duty of each authority to exercise of those functions, and the need to do all that it reasonably can, to prevent crime and disorder in its area.

Section 115 - any person who apart from this section would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority, shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of this Act.

8. Criminal Justice and Courts Services Act 2000

Section 67 - the authority for each area must establish arrangements for the purpose of assessing and managing the risks posed in that area by relevant sexual or violent offenders and other persons who have committed offences who are considered by the authority to be persons who may cause serious harm to the public.

Section 68 - interpretation of who is a relevant sexual or violent offender.

9. Education Act 1996

Section 322 - where it appears to a local education authority that any health authority or local authority could, by taking any specified action, help in the exercise of any of their functions under this Part, they may request the help of the authority, specifying the action in question.

10. Education Act 2002

Section 175 - A local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.

11. Health and Social Care Act 2001

Section 60 - gives the Secretary of State for Health powers to authorise use of identifiable information for essential medical purposes without the consent of patients.

12. **The Care Act 2014**

Adult safeguarding is the process of protecting adults with care and support needs from abuse or neglect (hereafter referred to as “adults”). It is an important part of what many public services do, but the key responsibility is with local authorities in partnership with the police and the NHS. The Care Act 2014 puts adult safeguarding on a legal footing and from April 2015 each local authority must:

- Make enquiries, or ensure others do so, if it believes an adult is subject to, or at risk of, abuse or neglect. An enquiry should establish whether any action needs to be taken to stop or prevent abuse or neglect, and if so, by whom.
- Set up a Safeguarding Adults Board (SAB) with core membership from the local authority, the Police and the NHS (specifically the local Clinical Commissioning Group/s) and the power to include other relevant bodies.
- Arrange, where appropriate, for an independent advocate to represent and support an adult who is the subject of a safeguarding enquiry or Safeguarding Adult Review (SAR) where the adult has ‘substantial difficulty’ in being involved in the process and where there is no other appropriate adult to help them.
- Cooperate with each of its relevant partners in order to protect adults experiencing or at risk of abuse or neglect.

13. **Learning and Skills Act 2000**

Section 114 - the Secretary of State may provide or secure the provision of services which he thinks will encourage, enable or assist the effective participation by young persons in education or training. In securing the provision of those services the Secretary of State may make arrangements with local authorities and other persons for the provision of services.

Section 120 - for the purpose of the provision of services in pursuance of section 114, any of the persons or bodies mentioned may supply information about a young person (a person who has attained the age of 13 but not the age of 20) to the Secretary of State or to any other person or body involved in the provision of those services. Those persons and bodies are a local authority, a health authority, the Learning and Skills Council for England, a chief officer of Police, a probation committee, a youth offending team and a Primary Care Trust.

14. **Local Government Act 2000**

Section 2 - councils have the power to do anything which is considered likely to achieve any one or more of their objectives.

- To promote or improve the economic wellbeing of their area.
- To promote or improve the social wellbeing of their area.
- To promote or improve the environmental wellbeing of their area.

15. **Management of Police Information (MOPI)**

Code of Practice on the Management of Police Information This code was developed under section 39 and 39a of the Police Act 1996 and enacted in November 2005. The code sets out principles governing the management of police information, including procedures governing authorised sharing of information obtained and recorded for policing purposes within the police service, and with other agencies. A full Manual of Guidance on the Management of Police Information supporting the requirements of the code was published in March 2006.

Policing purposes are defined in the code as:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice;
- any duty or responsibility of the Police arising from common or statute law.

The code allows the police to disclose police information to the other people or bodies where this is reasonable and lawful to do for the policing purposes as set out in Sub paragraph 2. Any sharing of information must comply with the ACPO Guidance on the Management of Police Information 2006 and any protocol, local or national, which may be agreed with the people or bodies needing to receive the information.

Additionally the ACPO/NIPD code of practice sets out obligations on people or receiving organisations police information to apply safeguards to protect the security and confidentiality of police information.

16. **National Health Service Act 2006**

Section 82 - in exercising their respective functions NHS bodies and local authorities must co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

Section 201 - a disclosure of information is made in accordance with this subsection if it is made for the purposes of any criminal investigation or proceedings.

17. **Access to Health Records 1990**

Under the Access to Healthcare Records Act 1990 and the Data Protection Act 1998, all patients have a right to request access to all their Healthcare Records. Persons wishing to access the records of a deceased individual may do so under the terms of the Access to Medical records Act 1990.

Providing access to medical records is essentially a confidentiality issue; therefore, the starting point is whether or not the patient has consented to disclosure. If not, access should be denied, unless there is some other clear justification for allowing access.

Disclosure with consent - Before allowing access to anyone other than the patient or colleagues involved in the patient's care, generally speaking, you will need to confirm that the person making the request has the patient's consent. You need to be clear about exactly what part of the record the consent applies to.

Disclosure without consent - Occasionally, there will be circumstances where you have to disclose a patient's records without their consent (and, rarely, in the face of the patient's clear objection to disclosure). There are three possible justifications for this:

- If you believe that a patient may be a victim of neglect or abuse, and that they lack capacity to consent to disclosure, you must give information promptly to an appropriate person or authority, if you believe disclosure is in the patient's best interests.
- You believe that it is in the wider public interest, or that it is necessary to protect the patient or someone else from the risk of death or serious harm. Examples of this might be to inform the DVLA if someone may be unfit to drive, or to assist the police in preventing or solving a serious crime, or informing the police if you have good reason to believe that a patient is a threat to others. You should follow GMC guidance (*Confidentiality*) on disclosure within the wider public interest.
- Disclosure is required by law – for example, in accordance with a statutory obligation, or to comply with a court order or a disclosure notice from the NHS Counter-Fraud Service. You have a duty to protect the confidential data of your patients under the Data Protection Act (1998) and civil monetary penalties can be imposed for serious contraventions of the act.

In any of these cases, you should only provide the minimum amount of information necessary to serve the purpose, and you should carefully document your reasons for making the disclosure.

18. 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.

19. Freedom of Information Act 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.

20. Safeguarding Vulnerable Groups Act 2006

The Safeguarding Vulnerable Groups Act 2006 (c 47) is an Act of the Parliament of the United Kingdom. It was created following the UK Government accepting recommendation 19 of the inquiry headed by Sir Michael Bichard, which was set up in the wake of the Soham Murders.

The Act establishes the legal basis for the Independent Safeguarding Authority who will manage the two lists of people barred from working with children and/or vulnerable adults replacing the current barred lists (List 99 the Protection of Children Act 1999 (PoCA), the scheme relating to the Protection of Vulnerable Adults (PoVA) and Disqualification Orders) The Act also places a statutory duty on all those working with vulnerable groups to register and undergo an advanced vetting process with criminal sanctions for non-compliance.

21. Mental Capacity Act 2005

The Mental Capacity Act (MCA) is designed to protect and empower individuals who may lack the mental capacity to make their own decisions about their care and treatment. It is a law that applies to individuals aged 16 and over. The MCA says:

- Everyone has the right to make his or her own decisions. Health and care professionals should always assume an individual has the capacity to make a decision themselves, unless it is proved otherwise through a capacity assessment.
- Individuals must be given help to make a decision themselves. This might include, for example, providing the person with information in a format that is easier for them to understand.
- Just because someone makes what those caring for them consider to be an "unwise" decision, they should not be treated as lacking the capacity to make that decision. Everyone has the right to make their own life choices, where they have the capacity to do so.
- Where someone is judged not to have the capacity to make a specific decision (following a capacity assessment), that decision can be taken for them, but it must be in their best interests.

- Treatment and care provided to someone who lacks capacity should be the least restrictive of their basic rights and freedoms possible, while still providing the required treatment and care.

22. 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.

23. 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.

24. 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

25. 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.

26. 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.

27. 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.hmsso.gov.uk/>

Appendix 2 – Data protection principles and the MAST/MASH

FIRST PRINCIPLE

The first data protection principle states you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.

The nature of the information that will be shared under this agreement will often fall below a statutory threshold of a Section 47 (Child Protection investigation) or even Section 17 Children Act 1989 (Child in Need). 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 obligations upon the police, local authorities, NHS bodies and others 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 piece of legislation gives the statutory power to share information for the purposes of this agreement.

DPA 2018 - Schedule 2 Part 1(2) Crime and taxation allows agencies to share information if complying with the fairness and transparency processing conditions (ie telling individuals how their data will be processed/shared) where it would be likely to prejudice the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or an imposition of a similar nature.

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. 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 MAST 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.

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.

The “Right to be Informed”

It is a requirement of the Data Protection Act 2018 that all organisations that process personal data should inform individuals how their data is to be processed. This is done via a Privacy Notice which will inform individuals about how their personal data will be used by that organisation. This notice will cover:

- i) The identity of the data controller.
- ii) Legal basis for processing the data or whether the processing is consent based
- iii) The purpose or purposes for which the data are intended to be processed.
- iv) Who the information will be shared with
- v) How it will be stored
- vi) Relevant transfers
- vii) Retention periods
- viii) Contact details for the DPO
- ix) Rights of individuals
- x) Any further information which is necessary, taking into account the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.

DPA 2018 - Schedule 2 Part 1(2) Crime and taxation allows agencies to share information if complying with the fairness and transparency processing conditions (ie telling individuals how their data will be processed/shared) where it would be likely to prejudice the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or an imposition of a similar nature.

Privacy Notices

Agencies agree to have adequate Privacy Notices in place, to notify data subjects of how and why their personal data may be shared.

Legitimate expectation

The sharing of the information by police fulfils a policing purpose, in that it will be done in line with policing principles 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, ensuring that any disclosure will be relevant, necessary and proportionate to the aims of this agreement, with any person or agency that will assist in fulfilling the policing purposes mentioned above.

Human Rights - Article 8: The right to respect for private and family life, home and correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention

of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

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

In pursuit of a legitimate aim –

The promotion of the welfare and wellbeing of children and ensuring they achieve all five outcomes is, by virtue of S.11 of Children Act 2004, a legitimate aim and major responsibility of the signatories to this agreement. The sharing of information under this agreement is also in line with Articles 2 and 3 of the Human Rights Act 1988, namely the right to life and the right to prohibition of torture or inhuman or degrading treatment.

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.

Schedule 2, Data Protection Act 2018

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 agreement 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".

Schedule 3, Data Protection Act 2018

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

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

SECOND PRINCIPLE

Lawfulness, fairness and transparency

You must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.

THIRD PRINCIPLE

Purpose Limitation

You must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.

FOURTH PRINCIPLE

Data Minimisation

You must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.

FIFTH PRINCIPLE

Accuracy

You must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.

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

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

SIXTH PRINCIPLE

Storage limitation

You must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business's circumstances and the reasons why you collect this data.

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 historic information for risk assessment purposes. However, once information is no longer needed, it should be destroyed.

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.

SEVENTH PRINCIPLE

Integrity and confidentiality

You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Under the terms of this agreement no information will be passed outside of the European Economic Area unless specific requirement exists and the originating organisation makes that decision for a particular reason in relation to the safeguarding of a child, young person or adult with a safeguarding need. Legal advice may be necessary in these cases.

Appendix 3 – Checklists for sharing information under the Data Protection Act 2018

Sharing personal information

- ☐ Do I have consent from the person?
- ☐ Do I have a contractual duty to share information?
- ☐ Is the sharing necessary to comply with a legal obligation?
- ☐ Is the sharing necessary to protect the individual's life or protect them from serious harm?
- ☐ Is sharing in the public interest or necessary for my organisation or the other organisation to undertake its official duties?
- ☐ Do I or the other organisation I want to share the information with have a legitimate and lawful purpose for sharing the information and, in my view the sharing would not cause unwarranted prejudice to the rights and freedoms of the individual?

This checklist derives from the conditions listed in Schedule 2 of the Data Protection Act 2018.

Sharing sensitive personal information

- ☐ Do I have explicit consent from the person?
- ☐ Does my organisation have a legal obligation in connection with employment e.g. to protect the health and safety of its staff?
- ☐ Is the sharing necessary to protect the life of the individual or someone else or to protect them from serious harm?
- ☐ Is sharing in the public interest or necessary for my organisation or the other organisation to undertake its official duties?
- ☐ Is the sharing necessary for medical purposes?
- ☐ Is the sharing in the substantial public interest
- ☐ Is the sharing for the purposes of preventing or detecting an unlawful act

This checklist derives from the conditions listed in Schedule 3 of the Data Protection Act 2018.

Sending personal information by post

- ☐ Mark post 'for the attention of the addressee only'
- ☐ Make sure envelopes and packages are effectively sealed and have the correct postage.
- ☐ Inform the designated recipient that the information has been sent and ask them to contact you if they do not receive it within the expected timeframe.
- ☐ Limit the amount of personal information disclosed to those details necessary for the recipient to carry out their role effectively.

Sending personal information by email

- ☐ Do not send the personal information by email unless you know the whole of the transmission is through fully secure networks.
- ☐ If you cannot use a secure e-mail account and must share the personal information electronically, ensure the correct e-mail address is clarified and consider what is the content of the information being shared.

Sharing personal information verbally

- ☐ Take care to ensure that your conversation cannot be overheard by others who do not need to know.
- ☐ Make sure you know who you are talking to over the phone and check that the individual is the right person to speak to.
- ☐ If you do not recognise the person calling, ask them for their name and their switchboard number and call them back using their organisations general number and not their direct office number, to ensure they are who they say they are.

Appendix 4 Letter to General Practitioners

Title

Address line 1

Address line 2

Address line 3

Town/city

Postcode

Date: DD/MM/YYYY

Dear Title,

This letter is a request for your consent for the MAST health practitioner to access your records if you are a SystmOne (S1) user.

The MAST in Calderdale significantly improves the sharing of information between agencies, helping to protect the most vulnerable children and young people from harm, neglect and abuse. It deals with all new safeguarding referrals about vulnerable children and young people, where someone is concerned about the safety or wellbeing of a child or young person, or think they might be being abused.

Within the MAST, information from different agencies is collated and risk assessed to decide what action to take. As a result, the agencies are able to act quickly in a co-ordinated and consistent way, ensuring that vulnerable children and young people are kept safe.

The MAST involves representatives from Calderdale Children's Social Care, Police and Health working together in the same location (Halifax Police Station). Virtual links exist to other services and agencies outside of the MAST such as Education, Housing, and Probation etc.

A request for Health information is always made to the MAST Health Team when a Health professional makes a referral. Health information provided by the MAST Health Team is proportionate to the referral details.

Consent to share health information is judged on each individual case; for some cases where there are concerns that the child maybe at significant risk of harm, consent from parent/carer will not be asked for. In the case of referrals where there are significant concerns, S1 records will be accessed by the MAST health team.

If, when a child is being discussed at a strategy meeting within the MAST, the GP does not use S1 and health information is scant, they will be called by the MAST Health Team and asked to provide relevant health information. This information needs to be provided in a timely manner. GP surgery staff should take the message and arrange for the duty doctor to call the MAST Health Team back and provide the MAST **Nurse Specialist** with any information.

If you would like further information or do not wish for your records to be accessed for this purpose please contact either Dr Paul Glover or Gill Poyser-Young or the MAST health team direct.

Yours **faithfully / sincerely,**

Gill Poyser-Young

Dr Paul Glover

Designated Nurse NHS Calderdale CCG

Named GP NHS Calderdale CCG






Appendix 5 Parties to this agreement

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

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

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

Agency	Post Held	Name	Signature	Date
Calderdale Council	SIRO/DPO	Tracie Robinson		19.3.19
Calderdale Council Children & Young Peoples Services	Service Manager	Zeljko Radevic		8.4.19
West Yorkshire Police Calderdale District	Chief Inspector, Partnerships and Neighbourhoods, Calderdale	Gareth Crossley		8.4.19
Locala CIC	Director of Nursing, Allied Health Professionals and Quality, Caldicott Guardian	Julie Clennell		19 March 2019
NHS Calderdale Clinical Commissioning Group	Chair	Steven Cleasby		

Date of Original Agreement	31 st July 2015
----------------------------	----------------------------

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

<https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>

The Seven Golden Rules to Information Sharing

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information,

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

To effectively share information:

- all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal
- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information **without consent**
- information **can be shared legally without consent**, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.
- relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Privacy Notice (Children's Social Care and Children's Services) Data Protection Act 2018

Collecting personal data

Calderdale Metropolitan Borough Council is the Data Controller for the purposes of the Data Protection Act. The information you provide helps us to support you and your family and meet our legal responsibilities, for example assessment of educational, social care or family support needs.

The data collected will include personal characteristics such as your name, date of birth, contact details, ethnic group and may also include any special educational needs or medical information. More detailed information is collected dependent on any need or services identified. We use the information to:

- Provide appropriate services, support and care to children and families;
- Assess whether our services are making a difference
- Develop and improve services
- Administer and protect public funds

Why we collect your data

We use your data to enable us to carry out our statutory functions and duties:

- Assess and identify any additional needs a child may have
- Provide interventions and services to children and families
- Provide a co-ordinated approach with other agencies to safeguard children
- To improve outcomes for children and reduce risk
- To comply with safeguarding policies and procedures

Who we share data with

We are required by law to pass on personal child data to the Department for Education (DfE), other Government departments and our partner organisations who use it to help with policy development, service delivery, performance management, funding and to assist with the development of good practice.

Wherever possible we will discuss with you the reasons for sharing information and ask for your consent. However, in some circumstances, when we feel that you or others are at risk, we may share information without your consent. When sharing information we do so in line with the Data Protection Act and agreed information sharing protocols across agencies that are providing services to the child and/ or family. Where information is received into a 'hub' arrangement all information is shared with the agencies that are part of that hub. i.e. Children's Social Care, Early Intervention, Police and Health are all partner agencies within the Multi-Agency Screening Team (MAST). This is the team that receives all contact/referrals for children residing in Calderdale where additional support or concerns is identified.

Storing your data

All information we record is stored securely and in accordance with the Data Protection Act 2018. The length of time we keep information varies depending upon different regulations. Your information will be kept for a maximum of:

- Early Intervention and referrals/assessments including Child in Need Planning is the DOB of the child + 25 years in line with education records
- Child Protection cases 40 years
- Children looked after 75 years

For more detailed information on the length of time we keep your data/information please refer to the contact details below.

Access to records

You have the right to see what information is held about you and to have incorrect data corrected. You do not have the right to have information removed unless it is incorrect as we are required by law and a statutory purpose to keep it.

If you have any queries about your records, or wish to see your records, please speak to the person who is working with you. Alternatively you can write to, or email, or phone the Information Management Team using the contact details below:

- Email information_management@calderdale.gov.uk
- Address Town Hall, Crossley Street, Halifax, HX1 1UJ
- Telephone 01422 392298

Complaints about data protection should be sent to the Councils Data Protection Officer (DPO) tracie.robinson@calderdale.gov.uk