

Response to Request for Information

Reference FOI 001345
Date 21 July 2017

Assessments and Support for Families

Request:

1. Please provide all documents, procedures, policies and / or protocols relating to data protection and information sharing held by the local authority in relation to assessments and support for families?
<http://www.wolverhampton.gov.uk/CHttpHandler.ashx?id=1514&p=0>
<http://www.wolverhampton.gov.uk/CHttpHandler.ashx?id=2307&p=0>
[See attached.](#)
2. Please confirm whether the LA consider that information obtained in a Children Act 1989 assessment is sensitive personal data as set out in section 2 of the Data Protection Act 1998?
[All assessments are confidential. EH Assessment/Social Work Assessment.](#)
3. What is the protocol to ensure confidential information is kept private when a Home Office worker attends a Children Act assessment? [See attached](#)
4. Please confirm whether the LA routinely seek consent from children/parents before sharing any information obtained in a Children Act assessment with the Home Office? Please provide all consent pro formas used for this purpose?
[See attached](#)
5. At the stage of seeking consent, are parents/children told that they can refuse consent, and of the consequences of refusal? Please confirm what is told to the parents / children. If there is a written document provided to them, please provide this to us. If not, please set out what it is that parents and children are told? [Consent guidance. Referral \(MARF\), Assessment and Plan Templates. MASH IG Guidance.](#)
6. If consent is refused what are the consequences? [See attached.](#)

Wolverhampton

Overarching Information Sharing Protocol

Version 1.9.2



Wolverhampton Homes



Version 1.9.2

Document references

Version	Version 1.9 Draft for final virtual sign off by WISG members
Date	March 2015
Author	Raz Bassi – Information Governance Lead- Royal Wolverhampton NHS Trust Anna Zollino-Biscotti – Senior Information Governance Officer – Wolverhampton City council

Change History

Version	Date	Description of change
1.0	June 2011	Draft
1.1	August 2011	Amendments to section 14. 4.1 following feedback.
1.2	September 2011	Amendments following feedback.
1.3	October 2011	Amendments to section 7.1 & 13.1 following feedback
1.4	October 2011	Amendments following feedback.
1.5	October 2011	Amendments following review by Dilys Jones Associates. Amendments also made to 14.2.
1.6	November 2011	WCC Legal sign off
1.7	December 2014	Review At WISG - Raz Bassi to incorporate feedback
1.8	Jan 2015	Comments added, circulated again for review. Changes to tier two and three templates.
1.9	March 2015	Final amendments made. Document circulated for Final Virtual sign off
1.9.1	April 2016	Updated with new signatories and Logos
1.9.2	June 2016	Updated with new/amended signatories and Logos

With Thanks to:

Wolverhampton City Council and its partners acknowledge the work that Kent & Medway undertook to produce this structure on which this document is based. This high level document has been jointly further developed by public sector organisations in Wolverhampton, to facilitate the sharing of information amongst key organisations.

Table of Contents

	Page
1.0 Executive Summary	4
2.0 Introduction	4
3.0 Purpose	5
4.0 Structure	6
5.0 Formal Implementation, Monitoring and Review	8
6.0 Organisations Covered by this Protocol	9
7.0 Legal Requirements and Professional Framework	10
8.0 Duties and Requirements of Parties	13
9.0 Agreement	20
10.0 Signatories	22
11.0 Appendix A 3 -Tier Information Sharing Structure	23
12.0 Appendix B Legal Considerations	24
13.0 Appendix C Relevant Legislation	26
14.0 Appendix D Consent Guidance Notes	37
15.0 Appendix E Handling Breaches	44
16.0 Appendix F Tier Two template - Information Community agreement	
17.0 Appendix G Tier three template - Purpose Specific Information Sharing Agreement Template	46

1 Executive summary

- This document is an overarching information sharing protocol for inter-agency information sharing within Wolverhampton. It does not impose any new obligations, but reflects current regulations and legislation.
- This protocol sets out the agreed standards that staff in public, voluntary and independent partner organisations must adhere to. It is intended to complement any existing professional Codes of Practice that apply to any relevant professionals working within partner agencies.

2 Introduction

- It is recognised that effective information sharing is required in order to enable organisations to improve client services, protect the public and respond to statutory requirements. Organisations also recognise the importance of having clear guidelines to follow and ensuring that this information is shared in a secure and confidential manner and in accordance with the law, including the Common Law of Confidentiality, the Data Protection Act 1998, the Human Rights Act 1998 and other related legislation and guidance. This overarching Information Sharing protocol (and appendices) comprises of a set of rules that the organisations identified in section 10 agree to comply with when sharing any personal information with another partner agency. It sets out the standards that staff must follow when sharing personal data to ensure that legislation is not breached and that confidentiality is maintained.
- The sharing of anonymised or purely statistical information is outside of the remit of this protocol, as the majority of legislation and rules concern only the sharing of personal information. However, the Purpose Specific Information Sharing Agreement (PSISA) template created under this protocol can be used to form a basis for the sharing of anonymised or statistical information.
- Signatories to this overarching protocol must be the highest level official within the partner organisation (e.g. Wolverhampton Council's Chief Executive). This high level commitment is recognition that information sharing is a key strategic objective of the partnerships within Wolverhampton.
- This Overarching Information Protocol (Tier 1) is the highest level in the protocol structure and applies to all sharing of personal information. Please refer to Section 4 – Structure, for an outline of the protocol structure.

3 Purpose

3.1. Overarching Objectives

To provide a robust policy framework for the legal, secure and confidential sharing of personal information between partner agencies within Wolverhampton, in order to enable them to meet both their statutory obligations and the needs and expectations of the people who they serve.

3.2. Strategic Objectives

- To deliver integrated public sector services in line with government initiatives and requirements,
- To facilitate the management and planning of effective and efficient services; and
- To enable parties to this Protocol to review, account for and improve on what they do through shared working and information sharing.

3.3. General Objectives

- Clarifies the legal background on information sharing
- Outlines the principles that are needed to underpin the process
- Provides practical guidance on how to share information in a series of supporting procedures
- Provides a framework within which organisations can develop Information Sharing Agreements between specific services or information communities.
- Includes arrangements for reviewing the use of this Protocol and for responding to breaches of this Protocol, any Information Community Agreements or Purpose Specific Information Sharing Agreements (PSISA).

4 Structure

4.1. Protocol Tier Structure

Tier 1 – Wolverhampton Overarching Information Sharing Protocol.

This document is a high-level policy document common to all organisations delivering health, social and community services, across Wolverhampton. It describes a common set of **principles** and defines the general parameters within which the signatory organisations will share information with each other. This document establishes ownership and transparent agreement to the spirit of information sharing in the best interests of service users and their families and carers, and it commits those who sign it to sharing information lawfully, ethically and effectively at all levels of their organisation. This Tier One document provides the context for the underlying tiers in the model.

The Overarching Policy is to be signed by Chief Executives (or equivalent) and by their Caldicott Guardians (or Designated Officers).

Tier 2 – Information Community Agreements

These documents are high-level agreements common to organisations delivering health, social and community services. They satisfy the Tier Two level of the Three-Tier Model for Information Sharing and focuses on the collective **purposes** underlying the sharing of information within the 'Information Community'. Tier Two documents describe common contexts and shared objectives between agencies delivering services of a similar scope. They reference the relevant underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information within the same Information Community. They also provide context for a supporting set of individual information sharing agreements (Tier 3) that determine at a detailed level, how personal information can be shared amongst organisations with the same information community.

Information Community Agreements are to be signed by Service Directors or the equivalent functional leads.

Tier 3 – Purpose Specific Information Sharing Agreements (PSISA)

These documents are the lowest level or third element of the Three-Tier model. These documents are aimed at an organisation's "operational management/practitioner" level and will define the relevant **processes** which support the information sharing between two or more agencies for a specified purpose. These documents will detail:

- What information is to be shared
- Why it is being shared (for what specific purposes)
- Who it is being shared with (between which agencies)
- When it is being shared (the times, the frequency etc)

- How it is being shared (format)

Purpose Specific Information Sharing Agreements (PSISA) are to be signed by Heads of relevant services who have the devolved local and/or operational responsibility for delivery.

4.2. 3-Tier Model for Information Sharing Diagram

To view the proposed 3-tier model, please refer to [Appendix A- 3-Tier Information Sharing Structure.](#)

5 Formal Implementation, Monitoring and Review

5.1. Approval

This Protocol will be formally signed off by the Chief Executive (or equivalent) for each of the partner agencies.

5.2. Adoption

- Formal adoption will follow as soon as 2 or more partners have signed this document. Agencies who sign the document will make their own arrangements for the publication of it on their individual internal and external websites, and for the internal operational implementation of this overarching document.
- Following implementation, this Protocol will be reviewed after 6 months. Thereafter it will be reviewed every year or sooner as legislation and guidance dictates. The reviews will be undertaken by Wolverhampton City Council (local Information Governance Officers) in consultation with the Caldicott Guardians and Data Protection/Information Governance Officers of the Partner agencies.
- This document then forms the basis for information exchanges between those agencies who have signed up. All partner agencies wanting to share personal data under this information sharing framework must sign this agreement.

5.3. Monitoring & Review

- Each of the partner agencies will have in place processes to audit and provide assurance in respect of compliance with all aspects of this Protocol and individual Purpose Specific ISAs that they have signed up to.
- Breaches of this protocol and subsequent Information Community Agreements or Purpose Specific ISAs will be managed according to the Procedures set out in [Appendix E -Handling Breaches.](#)

6 Organisations Covered by this Protocol.

Section 10 contains a list of the organisations who have signed up to this Overarching Information Sharing Protocol.

7 Legal Requirements and professional Framework

7.1. Understanding the legal framework for information sharing

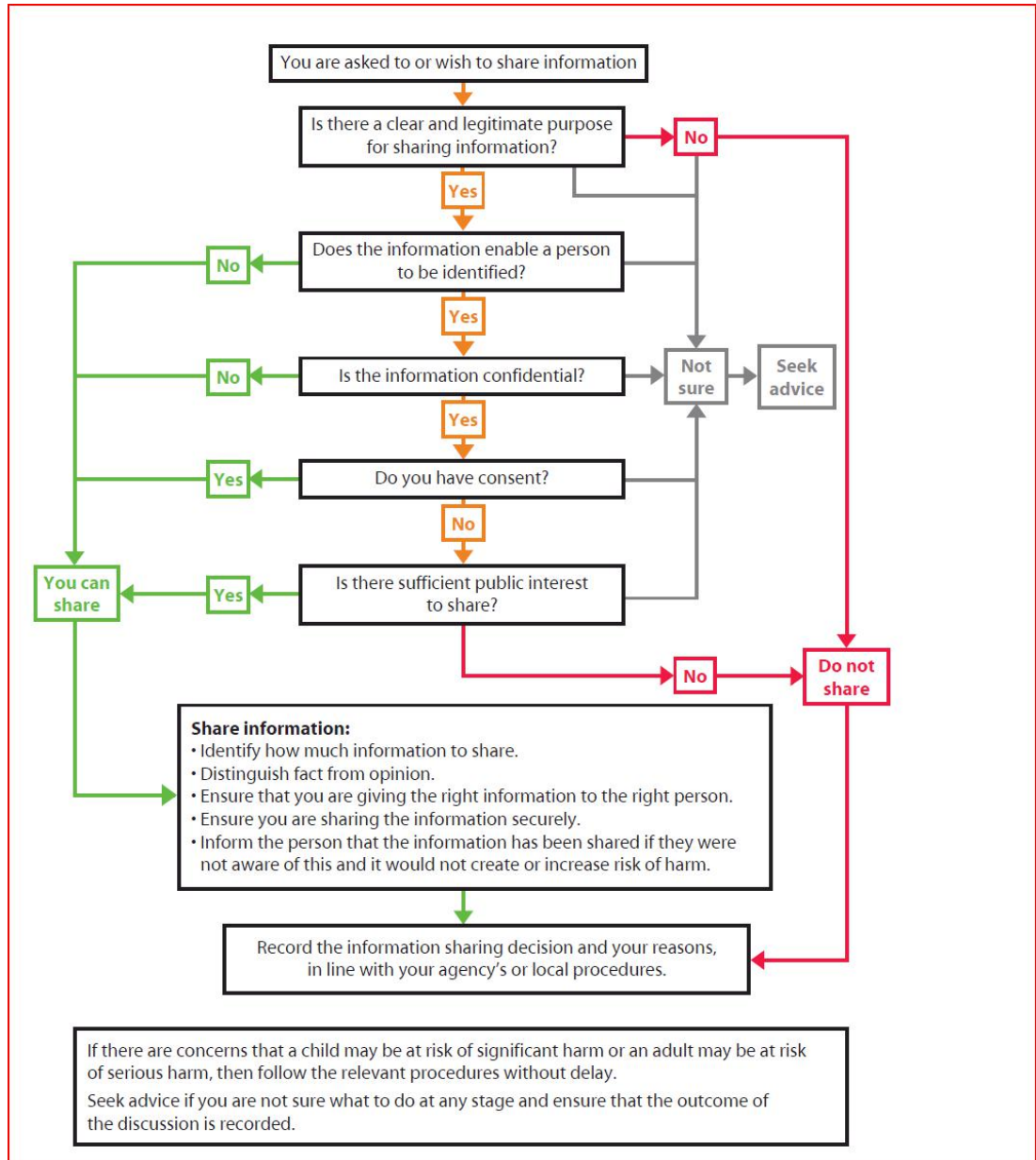
- The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.
- It is essential that practitioners sharing information are clearly aware of the legal framework within which they are operating.
- The purpose therefore of detailing the law within this protocol, is to highlight the legal framework that affects all types of personal information sharing, rather than to serve as a definitive legal reference point.
- This protocol has been developed in accordance with the ICO Data Sharing Code of Practice.
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx

7.2. How to approach questions around information sharing

- In order to approach questions around information sharing the protocol contains useful checklists and guidance notes (see appendices).
- [Appendix B - Legal Considerations](#) raises some of the questions in a more user-friendly way.
- In summary approaches to information sharing comes down to:
 - Establishing whether there is power to carry out the function to which the information sharing relates.
 - Checking whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of statutory, common law or other provisions.
 - Deciding whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim.
 - Decide whether the sharing of the data would breach any obligations of confidence.
 - Decide whether the data sharing could take place in accordance with the Data Protection Act 1998, with particular reference to the 8 Data Protection Principles.

- Following the Information Sharing Guidance for Managers and practitioners provided by HM Government; as detailed below in the Information Sharing Flowchart¹:

Key questions for Information Sharing.



¹ Information Sharing : Guidance for Practitioners and managers (HM Government 2006)

7.3. Freedom of Information Act (FOIA) 2000 requests

A number of the partner organisations are “public authorities” for the purposes of the Freedom of Information Act 2000 (FOI). This means that they could receive requests for information relating to the information sharing activities under this protocol or resultant purpose specific Information Sharing Agreement (e.g. statistics on the amount of data sharing being undertaken or the general nature of the data sharing). The public authority that receives the FOI request must make the other public authority aware of the nature of the request and their intended response.

8 Duties and Requirements of Parties

8.1 General undertakings by each agency

- A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing information appropriately.
- The sharing of information by organisations under this Protocol (and subsequent Information Community Agreements and Purpose Specific Information Sharing Agreement (PSISA)) will be based on the following principles:

8.1.1 **Commitment to sharing information**

Partner organisations recognise that multi-agency working sometimes requires a commitment to sharing personal information about service users in compliance with guidance and legislation.

8.1.2 **Statutory duties**

- Partner organisations are fully committed to ensuring that they share information in accordance with their statutory duties including the requirements of the Data Protection Act 1998, the Human Rights Act 1998 and The Common Law Duty of Confidentiality (see 8.1.4 below).
- Partner organisations recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and will adhere to the requirements of Schedule 3 of the Data Protection Act 1998 in respect of such information.

8.1.3 **Caldicott requirements**

All organisations recognise the requirements that Caldicott imposes on NHS organisations and Social Services Departments. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements:

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8.1.4 Duty of confidentiality

- Partner organisations recognise the importance of the legal duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are lawful grounds and an overriding justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.
- Agencies who are party to this Overarching Protocol will exercise caution when contemplating the disclosure of personal information relating to a deceased person. Although the Data Protection Act only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.
- All agencies who are party to this Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

- In the event of personal information that has been shared under this Overarching Protocol (and subsequent agreements) having or may have been compromised, whether accidental or intentional, the organisation making the discovery will without delay:
 - Inform the information provider (agency) of the details.
 - Take steps to investigate the cause.
 - If appropriate, take disciplinary action against the person(s) responsible.
 - Take appropriate steps to avoid a repetition.
 - Take appropriate steps where possible to mitigate any impact.

- On being notified that an individual's personal information has / have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary:
 - Notify the individual concerned,
 - Advise the individual of their rights,
 - Provide the individual with appropriate support.

- See [Appendix E - Handling Breaches](#) for more information.

8.1.5 **Consent**

- Where required, and unless legal exemptions are applicable, all agencies who are party to the Overarching Protocol will endeavour to seek informed consent from the individual concerned to share their personal information in accordance with an agreed Purpose Specific ISA.
- Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential to avoid the need to repeatedly seek consent over minor issues.
- In seeking consent to disclose personal information, the individual concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to withhold or withdraw consent.

For further guidance on consent, see [Appendix D - Consent: Guidance notes](#).

8.1.6 **Sharing without consent**

- Organisations will put procedures in place to ensure that decisions to share personal information without consent have been fully considered and comply with the requirements of the relevant law. Such decisions will be appropriately recorded for audit purposes. All relevant staff will be provided with training in these procedures.
- For further guidance see [Appendix D Consent: Guidance notes](#).

8.1.7 **“Need to know”**

Where it is necessary and permissible for information to be shared, this will be done on a “need-to-know” basis only. i.e. the minimum information, consistent with the purpose for sharing, will be given.

8.1.8 **Information kept confidential from the service user**

Where professionals request that information supplied by them be kept confidential from the service user, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on lawful grounds.

8.1.9 **Specific purpose**

- Partners will not abuse information that is disclosed to them under the specific purpose(s) set out in the relevant Purpose Specific ISA. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for their general use.
- Agencies wishing to use information for any purpose other than that for which it was originally provided, or who wish to disclose that information to any person other than those authorised to receive that information, must attempt to:
 - Inform the organisation that provided the information of their intention to use that information for a different purpose, and
 - Obtain explicit consent from the individual(s) concerned before processing such information (unless this is not practical – e.g. crime prevention purposes).
- Agencies who wish to use information that has been provided to them under a Purpose Specific ISA for research or statistical purposes must ensure that policies and procedures are in place to guarantee that such personal information is anonymised and in line with ethical standards.

8.1.10 **Fact / opinion**

Agencies who are party to this Overarching Protocol will ensure that their staff, who are authorised to make disclosure of personal information, will clearly state whether the information that is being supplied is either fact or opinion, or a combination of the two.

8.1.11 **Use of anonymised information where possible**

Personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is essential and appropriate. For all other purposes, information about individual cases that is to be shared will be anonymised. See diagram below for proposed uses for identifiable and di-identified information.

Class of data according to ICO code	Status of data	Description*	Legal basis required for processing?	Need to inform Public?	Conditions for onward disclosure
Anonymised	De-identified data for publication	Personal confidential data which has been anonymised with a low residual risk of re-identification. This means third parties can only re-identify the persons with unreasonable effort.	Not applicable	Desirable	No conditions for disclosure. Data may be published.
	De-identified data for limited disclosure or limited access	Personal confidential data that has been anonymised but with a residual high risk of re-identification. This means that the data does not identify persons on its own, but there is a significant risk that third parties could re-identify the persons with reasonable effort. A defining characteristic is a data set containing a single identifier such as NHS number or postcode**.	Legal basis requires safeguards that maintain anonymity. This means: <ul style="list-style-type: none"> • a contract that prevents re-identification; and • assured data stewardship arrangements***. Linkage of this data from more than one organisation for any purpose other than direct care must only be done in the Health and Social Care Information Centre OR an accredited safe haven.	Recommended	Either as de-identified data for publication OR to an environment covered by the same contractual arrangements as the disclosing party and confirmed data stewardship arrangements.
Identifiable	Personal confidential data	Personal confidential data that has not been through anonymisation and that may or may not have been redacted. Examples include: <ul style="list-style-type: none"> • any data set with greater than one direct identifier** OR • pseudonymised data with access to key for reversibility OR • pseudonymised data and holding one or more of source data sets in identified form. 	Legal basis for processing is required that meets the common law duty of confidentiality, Human Rights Act 1998 and Data Protection Act 1998. This means: <ul style="list-style-type: none"> • consent OR • statute OR • exceptionally on public interest grounds. Linkage of this data from more than one organisation for any purpose other than direct care must only be done in an accredited safe haven.	Required unless exempt	With consent for direct care OR under statute OR anonymised AND with appropriate contract or agreement***.

8.1.12 **Access to information**

- Individuals will be fully informed about the information that is recorded about them, who may see their information, for what purposes and their right to object to the relevant person within that organisation. Under the Data Protection Act they will normally be able to gain access to information held about them and to correct any factual errors that may have been made.
- If an agency has statutory grounds for restricting a person's access to information about themselves, they will normally be told that such information is held and the grounds on which it is has not been provided (unless this would prejudice an investigation or place an individual at risk).
- Information that has been provided by another agency under an agreed Purpose Specific Information Sharing Agreement (PSISA) may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent must be obtained prior to disclosure:
 - The provider has specifically stated that the information supplied must be kept confidential from the service user.
 - The information contains medical details.
 - The information is legally privileged.
 - The information is likely to prejudice the carrying out of social care duties.
- In the situation of two or more organisations having a joint (single) record on an individual, that individual may make their access to record request to any of the organisations. The organisation receiving the request will be responsible for processing the request for the whole record and not just the part that they may have contributed, subject to the conditions for disclosure mentioned above.
- Where an opinion about an individual is recorded and the individual feels the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and record their disagreement with the recorded opinion.

8.1.13 **Complaints procedures**

- Partner Organisations shall put in place procedures to address complaints relating to the disclosure of information. Partners must also ensure that service users are provided with information about these Complaint procedures.
- In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under an agreed Purpose Specific Information Sharing Agreement (PSISA), all agencies who are party to the Purpose Specific Information Sharing Agreement (PSISA) will provide co-operation and assistance in order to resolve the complaint.

8.1.14 **Ensuring minimum standards for all Purpose Specific Information Sharing Agreements**

- In order to maintain a consistent approach, all agencies who are party to this Protocol will ensure that any Purpose Specific Information Sharing Agreement (PSISA) will follow the framework set out in [Appendix F](#).
- Where information sharing protocols exist between agencies prior to signing up to the Overarching Protocol, such protocols will remain valid. However, such protocols should be reviewed and if necessary brought into line with the Wolverhampton 3-Tier Information Sharing Structure at the earliest opportunity in order to maintain a consistent approach.

8.1.15 **Disciplinary action**

Partner organisations will ensure that contracts of employment and/or relevant policies and procedures include reference to the issue of disciplinary action should staff disclose personal information on a basis which cannot be justified as reasonable in the particular circumstances (taking into account the purpose of the disclosure and any relevant statutes).

8.1.16 **Recording information disclosed under these protocols**

Agencies who are party to the Overarching Protocol will:

- Ensure that all personal information that has been disclosed to them under an agreed Purpose Specific Information Sharing Agreement (PSISA) will be recorded accurately on that individual's manual or electronic record in accordance with their policies and procedures.
- Put in place procedures to record not only the details of the information, but who gave and who received that information.

8.1.17 **Storage, transfer and destruction of personal information**

Agencies who are party to the Overarching Protocol will put in place policies and procedures governing:

- The secure storage of all personal information retained within their manual and/or electronic systems.
- The secure transfer of personal information both internally and externally. Such policies and procedures must cover:
 - Internal and external postal arrangements.
 - Verbally, face-to-face and telephone.

- Facsimiles (safe haven).
 - Electronic mail (secure network or encryption).
 - Electronic network transfer.
- The access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.
 - The retention and destruction of records containing personal information retained within their manual and/or electronic systems.

8.1.18 **Ensuring that staff under this protocol comply with their obligations**

Agencies who are party to the Overarching Protocol will ensure:

- That all staff are aware of, and comply with, their responsibilities and obligations with regard to the confidentiality of personal information about people who are in contact with their agency.
- That all staff are aware of, and comply with, the commitment of the organisations/agency to only share information legally and within the terms of an agreed Information Community Agreement or Purpose Specific Information Sharing Agreement (PSISA).
- That all staff are aware of, and comply with the commitment that information will be shared on a need-to-know basis only.
- That staff will be made aware that disclosure of personal information which cannot be justified, whether recklessly or intentionally will be subject to disciplinary action.

8.1.19 **Ensuring staff are trained to enable them to share information legally.**

- All parties to the Overarching Protocol will ensure that employees who need to share personal information under an Information Community Agreement or Purpose Specific Information Sharing Agreement (PSISA) are given appropriate training by their agency to enable them to share information legally, comply with any professional codes of practice and comply with any local policies and procedures.
- Staff who are not directly involved with sharing personal information should not be excluded from such training as it is possible that they may come across such information during the course of their duties. It may therefore be appropriate that such employees receive awareness training.

8.1.20 **Ensuring organisations signed up to this protocol can provide relevant assurances for data handling**

All organisations must have at least one of the following in place:

- ISO/IEC 27001:2005 an information security management
- Cyber essentials as per national guidance

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

- Minimum toolkit level 2 on the Information Governance Toolkit

9 Agreement

9.1 Purposes for which information will be shared

9.1.1 Overview

- Information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. However, each agency must have regard to its legal power in deciding whether they can share information for that particular purpose. The following range of purposes are agreed as justifiable for the transfer of personal information between the Partner Agencies as defined within the remit of this protocol:
 - Provision of appropriate care services
 - Assuring and improving the quality of care and treatment;
 - Improving the health of people in the local community
 - Monitoring, reporting and protecting public health;
 - Protecting children, young people and adults
 - Prevention of crime or disorder and the promotion of community safety
 - Supporting communities (geographical or otherwise)
 - Supporting people in need
 - Investigating complaints or potential legal claims
 - Compliance with court orders
 - Managing and planning services
 - Commissioning and contracting services
 - Developing inter-agency strategies
 - Performance management and audit
 - Research
 - Other statutory requirements

Please note that the above list provides an example of justifiable purposes for sharing information, however, the Data Protection Act 1998, Common Law Duty of Confidentiality and rights to privacy under the Human Rights Act 1998, still need to be considered.

9.1.2 Relevant information

Consideration must be given to the extent of any personal information that is proposed to be disclosed, taking into account the circumstances of the proposed disclosure. It may not be necessary to disclose all information held regarding a service user and only such information as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

9.2 Agreement

9.2.1 Indemnity

- Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.


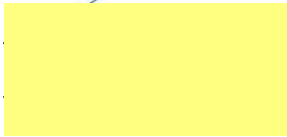




- Where a disclosing agency provides information to a requesting agency both parties shall assume that both the request and the disclosure are compliant with the requirements of the Data Protection Act 1998.
- If subsequently it is found that either the request for, or the disclosure of, information is in contravention of the requirements of the Data Protection Act 1998, the agency who originally breached the requirements of the Data Protection Act 1998, either in requesting or disclosing information, shall indemnify the other agency against any liability, cost or expense thereby reasonably incurred. However, this indemnity shall not apply:
 - Where the agency originally found to be in breach of the Data Protection Act 1998 did not know and, acting reasonably had no reason to know, that it had acted in breach of the Data Protection Act 1998 either in requesting or disclosing information
 - Unless either agency notifies the other agency as soon as reasonably practical of any action, claim or demand against itself to which it considers this indemnity may apply, permits the other agency to deal with the action, claim or demand by settlement or otherwise, and renders all reasonable assistance in doing so.

9.2.2 **The undersigned parties agree to:**

- Promote good practice in the sharing of personal information by ensuring compliance with the principles, purposes and processes of this Protocol.
- Take necessary action to identify and mitigate any breaches of the Protocol and to have established policies and practices for dealing with complaints about the sharing of information.
- Ensure that no restrictions are placed on sharing personal information other than those that are specified in this Protocol.
- Ensure that clients are informed of their rights in respect of personal information, including right of access and the complaints procedure.
- Develop systems of implementation, dissemination, guidance, training and monitoring to ensure that the Protocol is known, understood and followed by all professionals who need to share personal information.
- Establish processes to review the use of the Protocol, in order to ensure that practice is in accordance with the requirements of the Protocol, and to take corrective action as needed.
- Develop information processing systems that ensure collected data is complete, accurate, kept up-to-date and relevant.
- Ensure that collected data is stored and transmitted securely.

10 Signatories

This protocol will be signed by chief officers of the respective agency organisations on behalf of their organisations:

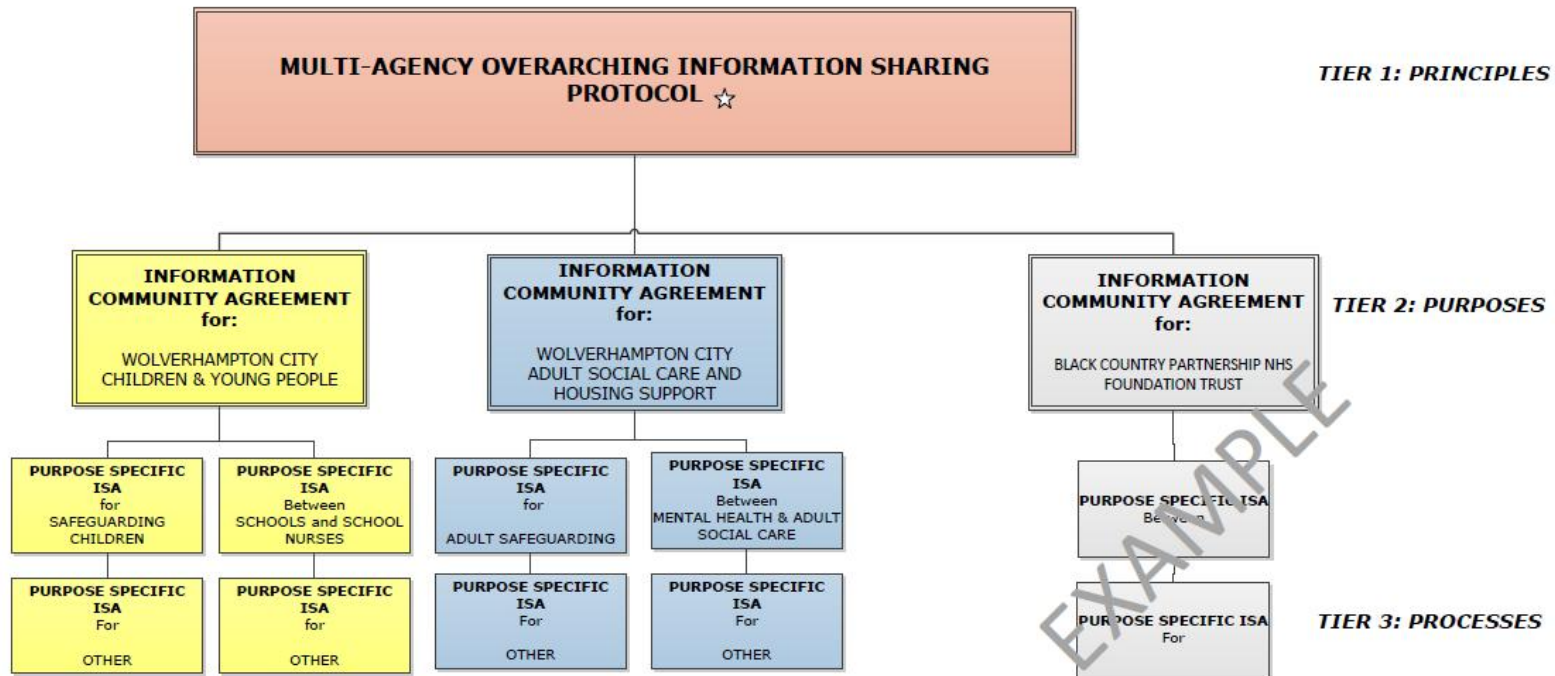
Organisation	Name of Signatory	Designation/Role	Date Signed
Wolverhampton City Council	Simon Warren 	Chief Executive	17 th November 2011
Staffordshire and West Midlands Community Rehabilitation Company (SWM-CRC)	J. Pejatta 	Assistant Chief Officer	7 th December 2015
Black Country Partnership NHS Foundation Trust	Paul Stefanoski 	Deputy Chief Executive, Director of Resources	17 th November 2011
NHS Wolverhampton CCG	Dr Helen Hibbs 	Clinical Accountable Officer	25 March 2015
The Royal Wolverhampton Hospital NHS Trust	David Loughten CBE 	Chief Executive	5 th December 2011
West Midlands Police	Neil Evans 	Chief Superintendent LPU Commander Wolverhampton	17 th November 2011
Wolverhampton Homes	Lesley Roberts	Chief Executive	5 th March 2012

Bushbury Hill Estate Management Board	Karen Williams [REDACTED]	Chief Officer	28 th March 2012
North Midlands (Neighbourhoods) Midland Heart Wolverhampton Office	Joanne Kelsall [REDACTED]	Operations Manager Midland Heart	25 th April 2012
Bromford Housing Group's	Phillipa Jones [REDACTED]	Executive Director and Company Secretary	9 th May 2012
Nehemiah Housing Group	Llewellyn Graham [REDACTED]	Chief Executive	18 th May 2012
Sanctuary Housing Association	Craig Moule [REDACTED]	Company Secretary	1 st June 2012
NACRO	David Watson [REDACTED]	Director of Justice and Health	3 rd March 2016

10.1 Signed copies of this document shall be retained by Wolverhampton Council's Data Protection/IG Officers.

11 APPENDIX A – 3-Tier Information Sharing Structure

THREE-TIER MODEL for INFORMATION SHARING



☆ Main agencies represented in multi-agency approach include Wolverhampton City Council, Royal Wolverhampton NHS Trust, Black Country Partnership Foundation Trust, West Midlands Police, Probation Services, Schools, Wolverhampton Homes, & Wolverhampton Voluntary Sector Council, Wolverhampton CCG.

12 Appendix B - Legal Considerations

12.1 Purpose

This is meant as a guide to assist in determining how to establish the legal basis for data sharing:

12.1.1 Vires issues

- Is the existing information that is to be shared subject to any statutory prohibitions whether express or implied?
- Even if there are no relevant statutory restrictions, do the bodies sharing the data have the vires to do so? This will involve careful consideration of the extent of express statutory, implied statutory and common law powers (see [Appendix C – Relevant legislation](#) for further detail on statutory powers).
- If there is no existing legal power for the proposed data collection and sharing, then, can the individual's consent to the disclosure be obtained?

12.1.2 Human Rights Act issues

- Is Article 8 of the European Convention on Human Rights (ECHR) engaged i.e. will the proposed data collection and sharing interfere with the right to respect for private and family life, home and correspondence? If the data collection and sharing is to take place with the consent of the data subjects involved, Article 8 will not be engaged.
- If article 8 of the ECHR is engaged, is therefore the interference:
 - in accordance with the law
 - in pursuit of a legitimate aim;
 - a proportionate response to the problem
 - necessary in a democratic society?

12.1.3 Common law duty of confidence issues

- Is the information confidential:
 - Does it have the necessary quality of confidence?;
 - Was the information in question communicated in circumstances giving rise to an obligation of confidence?;
 - Has there been unauthorised use of that material?
- Consider also whether the information has been obtained subject to statutory obligations of confidence. If the data collection and sharing is to take place with the consent of the data subjects involved, the information will not be confidential.

- If the information is confidential is there an overriding public interest that justifies its disclosure? The law on this aspect overlaps with that relating to Article 8 of the ECHR.

12.1.4 **Data Protection Act issues**

Please refer to [Appendix C – Relevant Legislation](#) when reading the following points:

- Does the DPA apply i.e. is the information personal data held on computer or as part of a “relevant filing system” or an “accessible record”?
- If the DPA applies, can the requirement of fairness in the First Data Protection Principle be satisfied?
- Can one of the conditions in DPA Schedule 2 be satisfied?
 - Paragraph 5 relating to public functions are of particular relevance to public sector data sharing;
 - Paragraph 6, relating to the balance between the interests of the data subject and the legitimate interests of the body that share and/or that receives the data.
- If the data are sensitive personal data can one of the conditions in Schedule 3 also be satisfied?
 - Paragraph, 7 which is in similar terms to paragraph 5 of Schedule 2, may be applicable.
- Can the requirement of compatibility that is in the Second Data Protection Principle be complied with?
- Do any of the exemptions that are set out in the Data Protection Act apply?

Seek advice from your organisation’s Data Protection Officer/Legal Advisor if unsure.

13 APPENDIX C - Relevant Legislation

13.1 List (non exhaustive) of legislation and other guidance that is of relevance to information sharing:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- The Mental Health Act 1983
- The Children Act 1989 (sections 17, 27, 47 and Schedule 2)
- The Children Act 2004 (sections 10, 11 and 12)
- The Care Act 2014
- The NHS & Community Care Act 1990
- The Access to Health Records Act 1990
- The Carers (Recognition & Service) Act 1995
- The Crime & Disorder Act 1998
- The Health Act 1999 (section 31)
- The Health and Social Care Act 2001 (Section 60)
- The Local Government Act 2000 (section 2)
- The Local Government Act 1972 (section 111)
- The Education Act 1996 (sections 10 and 13), The Education Act 2002 (section 175)
- The Learning and Skills Act 2000 (sections 114 and 115)
- The Crime and Disorder Act 1998 (section 115)
- The NHS confidentiality code of practice
- The Civil Contingencies Act (2004) Part 1 and supporting regulations.
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005
- The Equalities Act 2010

Some of the legislation is defined in greater detail below. For further advice on this legislation and other relevant professional guidance contact your organisations designated officer.

13.2 Introduction

- Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.
- In many instances legislation tends to use broad or vague statements when it comes to the matter of sharing personal information, for example: the agency is required 'to communicate, or will co-operate with' without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998.

- The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data). In general, recorded information held by public authorities about identifiable living individuals will be covered by the Data Protection Act 1998. It is important to take account of whether the information is held in paper records or in automated form (such as on computer or on a CCTV system): some of the provisions of the Data Protection Act 1998 do not apply to certain paper records held by public authorities. Broadly speaking, the eight data protection principles set out in Schedule 1 to the Data Protection Act 1998, and discussed further below, will apply to paper records held in a "relevant filing system" or an "accessible record", but not to other paper records.
- The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, providing that the necessary conditions of the Act can be met, sharing is perfectly legal. It is important to share information, when appropriate to do so, as to withhold it. Each information sharing episode needs to be assessed on its own merits.

13.2.1 **Administrative Law**

- The principles of administrative law regulate the activities of public bodies; these principles are mainly enforced by way of claims for judicial review in the courts. The courts do not generally review the merits of public law decisions but consider the legality, rationality or procedural propriety of decisions made by public bodies. The rules relating to illegality are most relevant to data sharing: a public body may not act in excess of its powers. If it does act in excess of its powers, then the act is said to be ultra vires. Acts within a public body's powers are said to be intra vires. Under the Human Rights Act 1998, an act of a public authority may be unlawful on the basis that it is contrary to the ECHR. Where questions involving the Convention are involved, the Court will need to consider the merits of the decision more closely than would be the case where the traditional administrative law principles are involved.
- Local authorities derive their powers entirely from statute and cannot act outside those limited statutory powers. Most of these statutory powers relate to specific local authority functions. In addition to these specific powers, section 111 of the Local Government Act 1972 provides that local authorities are empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions. Section 2 of the Local Government Act 2000 confers a wide (but not unlimited) power on local authorities to promote the well-being of their area.
- There is no general statutory power to disclose data, and there is no general power to obtain, hold or process data. As a result, it is necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied. Express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked. Alternatively it may be possible to rely on section 111 of the 1972 Act or section 2 of the 2000 Act as a basis for data sharing.

- The starting point in relation to implied powers or in relation to section 111 of the 1972 Act must be the power to carry out the fundamental activity to which data sharing is ancillary. If there is no power to carry out that fundamental activity then there can be no basis for implying a power to share data or for relying on section 111 of the 1972 Act.
- A statutory power must be exercised for the purpose for which it is created. If it is not, the exercise of the power will be ultra vires.

13.2.2 **Administrative powers**

- Express statutory powers: Express statutory powers can be permissive or mandatory.
 - Express permissive statutory powers (or gateways) to share data include section 115 of the Crime and Disorder Act 1998 (which allows persons to share information with relevant authorities where disclosure is necessary or expedient for the purposes of the Act) and regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (which, among other things, permits the Secretary of State to make particulars in the vehicle registration register available for use by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention). Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995, which makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 6 of the Audit Commission Act 1998, which imposes a legal obligation on the Council to provide relevant information to the Audit Commission.
- Local authorities are only able to do what is expressly or by implication authorised by statute. The following statutory powers are relevant, in addition to the specific powers mentioned above:
 - Section 111 of the Local Government Act 1972, which provides that a local authority has power to do anything, which is calculated to facilitate, or is conducive or incidental to, the discharge of any statutory functions.
 - Section 2 of the Local Government Act 2000, which provides that a local authority has power to do anything likely to achieve the promotion or improvement of the economic, social or environmental well-being of the area.

13.2.3 **Data Protection Act 1998**

- The key principles of the Data Protection Act are:
 1. Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions in schedule 3 of the Act.

2. Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).
3. Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
4. Personal Data shall be accurate and kept up to date.
5. Personal Data shall not be held for longer than is necessary.
6. Processing of Personal Data must be in accordance with the rights of the individual.
7. Appropriate technical and organisational measures should protect Personal Data.
8. Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient.

With few exceptions the Data protection Act 1998 requires anyone processing personal information to notify (register) with the Information Commissioner.

- The registration details include the type of information held, the purpose of use and who the information may be disclosed to. It is therefore essential that anyone considering sharing personal information establishes that their registration covers who they may disclose information to, or what information they may collect (when receiving shared information). If their registration does not cover these matters adequately, amendments must be registered with the Information Commissioner.
- The first and second principles of the Data Protection Act are crucial when considering information sharing. In essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should only be used for a purpose(s) compatible with the original purpose.
- Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully – For personal information to be processed lawfully, one of the conditions in Schedule 2 must be met. For sensitive personal information, one of the conditions in Schedule 3 must also be met.
- Sensitive information, as defined by the Act, includes information concerning a person's physical or mental health; sexual life; ethnicity or racial origin; political opinion; trade union membership; criminal record or details of alleged offences etc.
- In order for there to be no misunderstanding, on anyone's part, it is always advisable for the 'collector' of the information to ensure that the person is made fully aware of why the information is needed, what will be done with it, who will have access to it, their rights and if appropriate seek to inform consent of the individual concerned before sharing that information. This will usually be done via the use of Privacy Notices.
- There are circumstances where information can be shared even if informed consent has not been given. These include the following:

- Section 29 of the Act permits disclosure for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure.
- Disclosure is also permitted where information has to be made public, or where disclosure is required by law.
- For the purposes of the common law duty of confidentiality, if there is no informed consent, this is the point where the need for confidentiality would have to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests. See the more detailed discussion of confidentiality, below.
- For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered. See the more detailed discussion of Article 8, below.
- The Data Protection Act gives individuals various rights in respect of their own personal data held by others, namely the right to:
 - Access to their own information (subject access request).
 - Take action to rectify, block, erase or destroy inaccurate data.
 - Prevent processing likely to cause unwarranted substantial damage or distress.
 - Prevent processing for the purposes of direct marketing.
 - To be informed about automated decision taking processes.
 - Take action for compensation if the individual suffers damage.
 - Apply to the Information Commissioner or the court to have their rights under the Act enforced.
- Section 7 of the Act, gives an individual the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic).
- Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions (e.g. section 7(4) and the exemption provided by section 30 of the DPA).
- The Act provides the holder of the information a limited number of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the Act.
- The Data Protection Act 1998 does not apply to personal information relating to the deceased person.

The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from section 3.1.(f) which continues to provide a right of access to the health

records of deceased person made by their personal representatives and others having a claim on the deceased's estate.

In all other circumstances, disclosure of records relating to the deceased person should satisfy common law duty of confidence.

It is also worth noting that third party information that is held within a record of a deceased person is still covered by the Data Protection Act 1998, where the third party is still alive.

- **Schedule 2** of the Data Protection Act 1998 specifies conditions relevant for the processing of any personal data, namely:
 1. The data subject has given his/her consent to the processing, or
 2. The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract, or
 3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, or
 4. The processing is necessary to protect the vital interests of the data subject.
 5. The processing is necessary-for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions of a public nature exercised in the public interest by any person, or
 6. The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
- **Schedule 3** of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data. In addition to meeting a condition set out in schedule 2, at least one other condition must be met in schedule 3, namely:
 1. The data subject who the sensitive information is about has given his/her explicit consent, or
 2. The processing is necessary to comply with employment law, or
 3. The processing is necessary to protect the vital interests of the:
 - a. the individual, (where consent cannot be given or reasonably obtained), or
 - b. another person, (where the individual's consent has unreasonably been withheld), or

4. In the course of legitimate activities of specified non-profit organisations, and does not involve disclosing personal data to a third party unless the individual has consented. Extra limitations apply to this condition, or
5. The individual has deliberately made the information public, or
6. Processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights, or
7. Processing is necessary for administering justice, or for exercising statutory or government functions, or
8. Processing is necessary for medical purposes, and is undertaken by a health professional or someone who is subject to an equal duty of confidentiality, or
9. To monitor equality of opportunity, and is carried out with appropriate safeguards for the rights of the individual.

Further conditions relating to the processing of sensitive personal information are detailed in Data Protection (Processing of Sensitive Personal Data) Order 2000.

13.2.4 **Human Rights Act 1998 and European Convention on Human Rights**

- The Human Rights Act 1998 (the HRA) gives effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). In general, it is unlawful under the HRA for a public authority to act inconsistently with any of the Convention rights.
- Article 8.1. of the European Convention on Human Rights (given effect via the Human Rights Act 1998), provides that “everyone has the right to respect for his private and family life, his home and his correspondence.”
- This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.
- Article 8.2 of the European Convention on Human Rights provides “there shall be no interference by a public authority with the exercise of this right except 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.”
- In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s) to have taken a particular course of action:
 - that it has taken these rights into account;
 - that it considered whether any breach might result, directly or indirectly, from the action, or lack of action;

- if there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
 - (if qualified rights) whether the organisation has proceeded in the way mentioned below. “Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act”.

13.2.5 **Crime and Disorder Act 1998**

- The Crime and Disorder Act 1998 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 a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the Crime and Disorder Act. This power does not over ride other legal obligations such as compliance with the Data Protection Act (1998), the Human Rights Act (1998) or the common law duty of confidentiality.
- Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service, fire brigades 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.
- Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

13.2.6 **Common Law Duty of Confidentiality**

- All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.
- A duty of confidence arises when one person (the “confidant”) is provided with information by another (the “confider”) in the expectation that the information will only be used or disclosed in accordance with the wishes of the confider. If there is a breach of confidence, the confider or any other party affected (for instance a person whose details were included in the information provided) may have the right to take action through the courts.
- Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

13.2.7 Exemptions to the duty of confidentiality

- The duty of confidence is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed. These are as follows:
 - Disclosures with consent. If the person to whom the obligation of confidentiality is owed (whether an individual or an organisation) consents to the disclosure this will not lead to an actionable breach of confidence.
 - Disclosures which are required or allowed by law. “Law” in this context includes statute, rules of law, court orders etc.
 - Disclosures where there is an overriding public interest (e.g. to protect others from harm).
 - The courts have generally taken the view that the grounds for breaching confidentiality must be strong ones.
 - The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.
 - Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

13.2.8 Caldicott Principles

- Although not a statutory requirement, NHS and Social Care organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

13.2.9 Access to Health Records Act 1990

Within the governance structures and processes of healthcare organisations, Practitioners have been given professional accountability to protect specific 1st and 3rd party statements. This may include clinical assessments, diagnostics and results as well as sections of sensitive care plans and progress notes.

13.2.10 The Children Act 2004

- The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children. The key event, which led to these proposals for fundamental change, was the death of Victoria Climbié. This demonstrated that there were major flaws within the systems and structures for safeguarding and ensuring the welfare of children and young people.

Main provisions of the Act:

- A duty on agencies to co-operate to improve the well being of children and young people
 - A duty to safeguard and promote the welfare of children
 - A power to set up a new database with information about children
- Summary of the Children Act 2004

The following is a brief account of the key parts of the Act that specifically relate to the Change for Children programme in England.

Children's Services in England – Part 2

1. Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.
2. Section 11 creates a duty for the key agencies who work with children to put in place arrangements to make sure that they take account of the need to safeguard and promote the welfare of children when doing their jobs.
3. Section 12 allows further secondary legislation and statutory guidance to be made with respect to setting up indexes that contain basic information about children and young people to help professionals in working together to provide early support to children, young people and their families. Case details are specifically ruled out of inclusion in the indexes.

13.2.11 Civil Contingency Act 2004 – Part 1

This deals with information sharing between responder bodies, as identified in the Act, as a distinct duty under the Act and as a means of achieving other duties under the Act, and is summarised below:

- Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation.
- The initial presumption is that information should be shared, but that some information should be controlled if its release would be counter productive or damaging in some other way.
- There are various types of information. Information may be suitable for some audiences, but not for others. Also, the circulation of information can be limited to certain classes of organisation or individual.
- In most instances, information will pass freely between responders, as part of a more general process of dialogue and co-operation.

- However, a formal system exists to request information in circumstances where that is necessary.
- Information may also be accessible from open sources, and responders should endeavour to use this route as well.
- Not all information can be shared. Responders may claim exceptions in certain circumstances (and, as a result, not supply information as requested).
- Exceptions relate to sensitive information only. Where the exceptions apply, a responder must not disclose the information. (Readers of this document are advised to read Chapter 3 of the Guidance Notes to the Civil Contingency Act 2004)

14 APPENDIX D - Consent: Guidance notes

14.1 Consent

- 14.1.1 Consent issues can be complex and a lack of clarity can sometimes mean the information can be incorrectly shared. Consent can be “explicit” or implicit”. Obtaining explicit consent for information sharing is best practice therefore; it is recommended that where possible the consent sought should be explicit, obtained at the start of any involvement and appropriately recorded.
- 14.1.2 In order to facilitate the sharing of personal information (without specific statutory grounds) careful consideration should be given to obtaining explicit consent whenever possible, regardless of the person’s age.
- 14.1.3 For consent to be valid it must be:
- Fully informed – the individual is aware of what information will be shared, with whom and for what purpose.
 - Specific – a general consent to share information with “partner organisations” would not be valid. Specific means that individuals are aware of what particular information we will share, who with and for what purpose.
 - A positive indication by the data subject – the provision of opt outs on forms would therefore not obtain the consent of an individual.
 - Freely given – the individual is not acting under duress from any party.
- 14.1.4 The person giving the consent must also have the capacity to understand what they are consenting to.
- 14.1.5 Consent may be given verbally or in writing. In order to avoid any confusion or misunderstanding at a later date, verbal consent should be witnessed and the details of the witness recorded.
- 14.1.6 To give valid informed consent, the person needs to understand why their information needs to be shared, what type of information may be involved and who that information may be shared with.
- 14.1.7 The person should also be advised of their rights with regard to their information, namely:
- The right to withhold their consent.
 - The right to place restrictions on the use of their information.
 - The right to withdraw their consent at any time.
 - The right to have access to their records.

- 14.1.8 As well as discussing consent with the person, it is seen as good practice that the person should also be given such information in another required format e.g. different language, Braille.
- 14.1.9 In general, once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent.
- 14.1.10 If a person makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for disclosing without consent (see 13.9 below).
- 14.1.11 A person, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusal, their wishes must be respected unless there are sound legal grounds for not doing so.
- 14.1.12 If a person refuses or withdraws consent, the consequences should be explained to them, but care must be exercised not to place the person under any undue pressure.
- 14.1.13 In the Purpose Specific Information Sharing Agreement (PSISA), detail must be provided on when and how often individuals are reminded of the fair processing notice (and in effect given the chance to withdraw the consent that they have previously provided).
- 14.1.14 New consent will be required where there are to be significant changes to:
- the personal data that will be shared,
 - the purposes for which it will be shared, or
 - the partners involved in the sharing (i.e. the proposed data sharing is not covered by the original fair processing notice which states which agencies information will be shared with).

14.2 Capacity to consent

- 14.2.1 For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process.

All people aged 16 and over, are presumed in law, to have capacity to give or withhold their consent to sharing of confidential information unless, there is evidence to the contrary. Having mental capacity means that a person is able to make their own decisions. The Mental Capacity Act says that a person is unable to make a particular decision if they cannot do one or more of the following four things:

- Understand the information given to them
- Retain that information long enough to be able to make the decision
- Weigh up the information available to make the decision

- Communicate their decision – this could be by talking, using sign language or even simple muscle movements such as blinking an eye or squeezing a hand.

The Mental Capacity Act 2005 Code of Practice provides information on points to consider when assessing a person's capacity to make a decision and should be referred to for more detailed guidance.

<http://www3.imperial.ac.uk/pls/portallive/docs/1/51771696.PDF>

14.3 Young Persons

14.3.1 Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.

14.3.2 The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent.

14.3.3 It should be seen as good practice to involve the parent(s) of the young person in the consent process, unless this is against the wishes of the young person.

14.4 Parental Responsibility

14.4.1 The Children Act 1989 sets out persons who may have parental responsibility, these include:

- The child's parents if married to each other at the time of conception or birth;
- In the case of children born after 1 December 2003, where the father's details are registered on the birth certificate the father will also have parental responsibility.
- The child's mother, but not the father if they were not so married and not named on the child's birth certificate (as above), unless the father has acquired parental responsibility via a court order or a parental responsibility agreement or the couple subsequently marry;
- The child's legally appointed guardian;
- A person in whose favour the court has made a residence order in respect of the child;
- A local authority designated in a care order in respect of the child:
- A local authority or other authorised person who holds an emergency protection order in respect of the child. (Note: Foster parents or guardians do not automatically have parental responsibility)

14.5 Whilst, under current law, no-one can provide consent on behalf of an adult in order to satisfy the Common law requirement, it is generally accepted by the courts that decisions

about treatment, the provision of care, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

14.6 Obtaining Consent

14.6.1 For consent to be valid a number of criteria must be satisfied (see 13.1.3 above). In order for consent to be obtained lawfully it is essential that all persons who may be expected to obtain consent for the sharing of personal information receive appropriate training and that under normal circumstances only those employees who have received training and been approved by management should seek consent.

14.7 Disclosure of Personal Information

14.7.1 The passing of personal information without either statutory power or the consent of the person concerned, places both the agency and the individual member of staff at risk of litigation.

14.7.2 It is therefore essential that all agencies who are party to the Overarching Protocol have in place policies and procedures governing who may disclose personal information and that such policies/procedures are communicated to all of their employees.

14.8 Disclosure with consent

14.8.1 Only staff who have been authorised to do so should disclose personal information about an individual service user.

14.8.2 Prior to disclosing personal information about an individual, the authorised member of staff should check the individual's file/record in order to ascertain:

- that consent to disclose has been given, and
- the consent is applicable for the current situation, and
- any restrictions that have been applied.

- 14.8.3 On the first instance of disclosure with respect to the particular situation, the person making the disclosure should notify the recipient if consent has been given for the disclosure and any specific limitations the individual has placed on their consent.
- 14.8.4 Disclosure of personal information will be strictly on a need to know basis and in accordance with any Information Community Agreement and/or Purpose Specific Information Sharing Agreement (PSISA).
- 14.8.5 All information disclosed should be accurate and factual. Where opinion is given, this should be made clear to the recipient.
- 14.8.6 On disclosing personal information to another agency, a record of that disclosure should be made on the individual's file/record, this should include:
- When the disclosure was made
 - Who made the disclosure
 - Who the disclosure was made to
 - How the disclosure was made
 - What was disclosed
- 14.8.7 The recipient of information should record:
- The details of the information received
 - Who provided it
 - Any restrictions placed on the information that has been given

14.9 Disclosure without consent

- 14.9.1 Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.
- 14.9.2 There are exceptional circumstances in which a service user's right may be overridden, for example:
- Where there is evidence or reasonable cause to believe that a child, young person or adult is suffering or risk of suffering, significant harm, or
 - if there is evidence of serious public harm or risk of harm to others, or
 - if there is evidence of a serious health risk to an individual, or

- if the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime.
 - if instructed to do so by a court
- 14.9.3 All agencies should designate a person who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person should hold sufficient seniority within the agency with influence on policies and procedures. Within the health and social care agencies it is expected that this person will be the Caldicott Guardian.
- 14.9.4 If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.
- 14.9.5 A record of the disclosure will be made in the service user's case file and the service user must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed. If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection work) where it may not be appropriate to inform the service user of the disclosure of information. This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the service user of such disclosure. In many such situations it will not be a case of never informing the service user, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the service user's case file, clearly stating the reasons for the decision, and the person making that decision.
- 14.9.6 In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.
- 14.9.7 All agencies who are party to this Overarching Protocol should set in place policies and procedures that deal specifically with the sharing of information under emergency situations e.g. major disaster.
- 14.9.8 If disclosure is made without consent, the person making the disclosure must:
- Advise the recipient accordingly.
 - Record the full details of the disclosure that has been made, including the reason why the decision to disclose was taken (statute or exemption);
 - Who made the disclosure and to whom it was disclosed to.
- 14.9.9 The recipient of information that has been disclosed without consent should record:
- The details of the information received.

- Who provided it.
- Any restrictions placed on the information that has been given e.g. 'not to be disclosed to the service user'.
- That the information was provided without consent, and the reason(s) why (if known).

14.10 Recording Consent

14.10.1 All agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

14.10.2 The consent form should indicate the following:

- Details of the agency and person obtaining consent.
- Details to identify the person whose personal details may/will be shared.
- The purpose for the sharing of the personal information.
- The organisation(s)/agency(ies) with whom the personal information may/will be shared.
- The type of personal information that will be shared.
- Details of any sensitive information that will be shared.
- Any time limit on the use of the consent.
- Any limits on disclosure of personal information, as specified by the individual.
- Details of the supporting information given to the individual.
- Details of the person (guardian/representative) giving consent if appropriate.

14.10.3 The individual or their guardian/representative, having signed the consent, should be given a copy for their retention.

14.10.4 The consent form should be securely retained on the individual's file/record and that relevant information is recorded on any electronic systems used in order to ensure that other members of staff are made aware of the consent and any limitations.

15 APPENDIX E - Handling Breaches

The process for reporting breaches of this Protocol (Tier 1), any Information Community Agreement (Tier 2) and other Purpose Specific Information Sharing Agreement (PSISA) (Tier 3) is outlined below.

15.1 All breaches are to be logged, investigated, and the outcome noted. The logs will be examined as part of the review process.

15.1.1 The following types of incidents will be logged:

- Refusal to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- Disclosure of information to members of staff who do not have a legitimate reason for access
- Non-delivery of agreed reports
- Inappropriate or inadequate use of procedures e.g. insufficient information provided
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements.

15.2 Breaches noted by members of staff:

15.2.1 A member of staff working on behalf of any organisation party to this protocol who becomes aware that the procedures and agreements set out in the protocol (or subsequent agreements) are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the protocol.

15.2.2 The manager should record the issue and check whether the concern is justified. If the manager concludes that the protocol is being breached, he or she should first try to resolve it informally. If the matter can be resolved in this way, the outcome should be noted and forwarded to the designated person for that Information Community Agreement or Purpose Specific Information Sharing Agreement (PSISA) who should file the details in a 'breaches log'.

15.3 Breaches alleged by a member of the public:

15.3.1 Any complaint received by, or on behalf of, a member of the public concerning allegations of inappropriate disclosure of information will be dealt with in the normal way by the internal complaints procedures of the organisation who received

the complaint: Any disciplinary action will be an internal matter for the organisation concerned.

- 15.3.2 In order to monitor adherence to and use of the protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information is passed by the officer designated to deal with breaches of the Purpose Specific Information Sharing Agreement (PSISA). The designated officer should report any complaints of this nature to the equivalent officer in each agency.
- 15.3.3 All alleged breaches of the protocol, whether proven or not, should be analysed as part of the formal review of this protocol and subsequent Information Community Agreements or Purpose Specific Information Sharing Agreement (PSISA)s.
- 15.3.4 The ICO has produced guidance on data security breach management. In the event of a data breach occurring, each will be managed on a case by case basis, in accordance with this guidance. This guidance will also be followed where a decision is required regarding notification of the data breach to the ICO.

16 APPENDIX F – Template Tier Two – Information Community agreement

To follow – April 2015

17 APPENDIX G - Purpose Specific Information Sharing Agreement (PSISA): Template

Note:

THIS TEMPLATE IS IN DRAFT FORMAT AND ILLUSTRATES THE TYPE OF INFORMATION THAT NEEDS TO BE CONSIDERED WITHIN A TIER 3 DOCUMENT. AT THIS DRAFT STAGE, TITLES AND LAYOUT MAY BE SUBJECT TO CHANGE.

PURPOSE SPECIFIC INFORMATION SHARING AGREEMENT (PSISA)

The Agreement

TITLE:

Document History

This document has been distributed to:

Version	Date	Author	Released to	Comments/Changes made

Links to other Information Community Agreements or Purpose Specific Information Sharing Agreement (PSISA)s:

Agreement Title	Date & Version	Lead Agency	Contact details

Template

Please refer to the accompanying guidance notes when completing this form.

1 What category of data under the Data Protection Act is being shared?	YES/NO
Data to be shared is classified as Personal Data	
Data to be shared is classified as Sensitive personal Data	
Data to be shared will be anonymised	
Data to be shared will be psuedonymised	

2 Who will I be sharing information about?

3 For what purpose is the information being shared?	
Is the information being shared for Primary Purposes	YES/NO
Is the information being shared for secondary purposes	YES/NO

4 What information will be shared?

(A) Description of data/information:	(B) Field:	(C) Extracted from which system/Derived from:	(D) Agency Name:

(E) Frequency of data sharing	One off: Y/N	Routine: Y/N
(F) Other relevant information:		

5 Who might I be sharing with?

Agency & Lead Contact details:	Provider	Recipient

6 Can I legally share this information?	
(A) Legislation	(B) Duties
(C) Data Protection Act 1998	<p>Under Schedule 2 of the DPA, either of the following conditions can be met:</p> <p>1.</p> <p>Under Schedule 3, the following conditions can be met:</p> <p>1.</p> <p>It is also important to ensure that other Data Protection principles are complied with, for example the information being shared is relevant to the purposes of this agreement and is not excessive; information being shared is accurate and up to date; information is kept for no longer than necessary; information shared is kept secure.</p>

7 Do I need to obtain consent?	
(A) Are you relying an on implied statutory power to share?	Y/N
(B) Are you relying on consent?	Y/N

8 What am I telling Service Users about this information sharing & how are they notified?	
(A) Is the information being shared for a different purpose other than that set out in each agency's fair processing notice on how we use information?	Yes – go to A1 No – go to B
(A1) Provide the link to each Agency's privacy notice	
(B) How will individuals be notified of the data sharing under this agreement?	

9 How and when might I share information?

(A) Role/ person sending/receiving data	(B) Organisation	(c) Method of Secure Transfer	(D) Frequency of Transfer

10 How will shared information be recorded and held?

(A) Organisation	(B) Location/Technical arrangements	(C) Duration	(D) Destruction

11 Who else can access this information?

--

12 Handling Breaches	
(A) Name and contact details of person who is to be informed of breach	
Agency	Name and contact details
(B) Timescales	

13 Other measures or considerations

14 Review of this agreement	
Name/Role of Reviewers:	
Date of Initial Review	
Date of Consequent Reviews:	

Annex 1

Purpose Specific Information Sharing Agreement (PSISA)

In respect of

(Insert Title)

DECLARATION OF ACCEPTANCE & PARTICIPATION

Signed by, for and on behalf of: Page 1 of

Organisation	
Name	
Position	
Contact Details: Phone: Email:	
Signature:	
Date:	

Name of agency contact for sharing information under this Purpose Specific Information Sharing Agreement (PSISA)	
Position	
Contact Details: Phone: Email:	
DPA Registration Number & Date of Renewal:	

Each agency who signs up to this agreement is to complete this form. Please print off as required.

Annex 2

Purpose Specific Information Sharing Agreement (PSISA)

(Insert Purpose Specific Information Sharing Agreement (PSISA) Title)

Master List of Signatory Organisations & their Designated Person's

Page 1 of

Agency	Designated Person & Position	Contact Details (telephone & Email Address)	Date when agency signed up to this PSISA

Please insert, complete and print additional sheets as required.

Purpose Specific Information Sharing Agreement (PSISA) – Guidance Notes

General

See Wolverhampton Overarching Information Sharing Protocol – **Section 4 - Structure** for an overall description of the Information Sharing three tier approach and the different elements.

In order to share appropriate information between partners there must be a lawful, defined and justifiable purpose(s) which supports the effective delivery of a policy or service that respects people’s expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This in turn must be supported by robust business processes.

The questions in this document are designed to ‘walk’ Managers/Practitioners/Designated Person’s and other specialist support (e.g. Legal, Technical, Data Protection, etc) through a process that should help fulfil this objective.

Scope

- This Purpose Specific Information Sharing Agreement (PSISA) is the third element of the information sharing framework. It is aimed at an organisations “operational management/practitioner” level and it will define the relevant business processes which support information sharing between two or more agencies for a specified purpose.
 - Those Managers/Practitioners/Designated Persons negotiating this Purpose Specific Information Sharing Agreement (PSISA) will have to complete Sections 2 to 14 inclusive.
 - This Purpose Specific Information Sharing Agreement (PSISA) is supplementary to Wolverhampton Overarching Information Protocol (Tier 1), which must be consulted when drawing up this agreement, along with any Information Community Agreements that are in place and relevant to this Purpose Specific Information Sharing Agreement (PSISA).
- Partner organisations may belong to a variety of differing Purpose Specific Information Sharing Agreement (PSISA)s and Information Community Agreements.

Partners may use the information disclosed to them under a Purpose Specific Information Sharing Agreement (PSISA) only for the specified purpose(s) set out in that Purpose Specific Information Sharing Agreement (PSISA) document. They may not regard shared information as intelligence for the general use of their organisation unless they have defined and agreed this purpose within the Purpose Specific Information Sharing Agreement (PSISA) and have informed their respective service users of this use.

- Wherever this Purpose Specific Information Sharing Agreement (PSISA) impacts, or has a dependency, on another Purpose Specific Information Sharing Agreement (PSISA) then details of these must be entered into the Table at Section 2 of this document.

Parties to this Purpose Specific Information Sharing Agreement (PSISA)

- The parties to the Purpose Specific Information Sharing Agreement (PSISA) are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document (See this Document Annex 1). This list, along with the details of each organisation's 'Designated Person(s)' as shown on the 'DAP' and at Annex 2, will be updated and reissued on a regular basis.
- Any party to this Purpose Specific Information Sharing Agreement (PSISA) who is not already a party to Overarching Protocol, agrees to comply with the terms of the Overarching Protocol insofar as it is relevant to the information sharing under this Purpose Specific Information Sharing Agreement (PSISA).
- By signing this document all of the parties agree to accept and implement this Purpose Specific Information Sharing Agreement (PSISA) and to adopt the statements and procedures contained within it.
- Any purported breaches of, or other complaints about, this agreement will be dealt with in accordance with the processes described at [Appendix E - Handling Breaches](#) of the Overarching Protocol.

User Guide

1 What category of data under the Data Protection Act is being shared?

Please select the category of data being shared.

- Personal Data – information that would identify a living individual such as name, date of birth, address etc.
- Sensitive Personal Data – personal data which consists of the following information:
 - The racial or ethnic origin of an individual
 - Political opinions
 - Religious beliefs or beliefs of a similar nature
 - Membership of a trade union
 - Physical or mental condition of an individual
 - Sexual life of an individual
 - The commission or alleged commission of an offence or
 - Any proceedings for any other offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.
- Anonymised Data – data which has had identifiers removed so that an individual cannot be identified.
- Pseudonymised Data – data which has had identifiers removed and replaced with a pseudonym.

The data being shared under this agreement is likely to be either personal or personal sensitive data, unless the information to be passed is entirely anonymised or statistical. Where if it is anonymised or statistical, you should give careful consideration to the possibility that an individual could nevertheless be identified from it – e.g. if it provides statistics on the ethnicity of crime victims in a limited geographical area it might inadvertently identify someone from an uncommon ethnic group in that locale. Pseudonymised information may be a consideration in these circumstances.

2 Who will I be sharing information about?

Please detail the types of service users whose information is being shared.

3 For what purpose is the information being shared?

Provide detail on the specific purpose for which personal information will be shared and the benefit that is to be achieved by sharing the information.

Please indicate whether the information sharing is for PRIMARY or SECONDARY PURPOSES.

Primary Purposes – this is information that is being shared for direct healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

Secondary Purposes – this is information being shared for non-direct healthcare and medical purposes - such as service improvement, performance management, reporting or commissioning.

4 What information will be shared?

- (A) List the items of information to be disclosed - for example Name, DOB, Address, Postcode,
- (B) List the data field name/criteria each item will be derived from.
- (C) List the system(s) from which each data field/record is extracted from/derived from
- (D) List the Agency from where the information is being sent from.
- (E) Detail the frequency of when the information is being sent. Is the information being shared as a one-off data sharing initiative - if so detail when the information is being sent. Is the information being shared on a routine basis – if so detail the frequency. If on the other hand you propose an agreement to make a series of individual disclosures in response to specific requests – sharing offender details at case conferences for instance -it may be necessary to be more general.
- (F) Are there any data quality issues, such as the accuracy, validity, timeliness and relevance of the data, if there are, then these should be considered here.

5 Who might I be sharing with?

Identify the relevant agencies/ organisations/practitioners and whether they are a provider or recipient of personal information or both.

6 Can I legally share this information?

Does your organisation have the vires (power) to share? Which particular legislative function is the data sharing taking place?

- (A) List the legislation/statutory duty that the information can be shared under.
- (B) List the relevant section and statutory duties that enable the sharing to take place.
- (C) Under the Data Protection Act 1998, what conditions in schedule 2 and/or schedule 3 of the Act can be met? If personal data is being shared then only 1 condition from schedule 2 needs to be met. Where sensitive personal information is being shared – then 1 condition from both schedule 2 and 3 need to be met.

Conditions for processing personal data under the DPA 1998.	
<i>Schedule 2 - Personal Data</i>	<i>Schedule 3- sensitive personal data</i>
The individual who the personal data is about has consented to the processing.	The individual whom the sensitive personal data is about has given explicit consent to the processing.
For the performance of a contract to which the 'individual' is a party, or the individual has	The processing is necessary so that you can comply with employment law.

asked for something to be done so they can enter into a contract	
The processing is necessary because of a legal obligation that applies to the agency (except an obligation imposed by contract)	The processing is necessary to protect the vital interests of: - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or - another person (in a case where the individual's consent has been unreasonably withheld).
The processing is necessary in order to protect the vital interests of the data subject. This applies in cases of life or death, such as where an individual's medical history is disclosed to A&E treating the data subject following a serious road accident.	The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
The processing is necessary for exercising statutory, governmental, or other public function	The individual has deliberately made the information public
The processing is in accordance with "legitimate interests" condition	The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
	The processing is necessary for administering justice, or for exercising statutory or governmental functions.
	The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality
	The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

See [Appendix B and C](#) of the *Wolverhampton Overarching Information Sharing Protocol* for further guidance.

7 Do I need to obtain consent?

- (A) Are you relying on an expressed or implied statutory power to sharing? Refer to section 6 - is there a statutory power or legal duty that enables you to share information without consent? What conditions for processing are being met for the data you are sharing?
- (B) Are you normally going to rely on consent? If so describe how consent will be obtained, recorded and how long it will be valid for.

If consent is normally required to share information for this purpose; provide detail on any specific circumstances where this consent is not required.

Advice on consent is available from [Appendix D](#) in the Wolverhampton Overarching information sharing protocol

8 What am I telling Service Users about this information sharing & how are they being notified?

- (A) Identify whether the sharing of information under this agreement is covered by each relevant agency's "fair processing notice"/Privacy Notice (See Appendix D – 13.1.6 and 13.1.7 of the Wolverhampton Overarching Information Sharing Protocol).
- (B) If the sharing of data is not covered under this agreement complete section B and describe how you are informing individuals of the data sharing under this agreement.

Also outline how and when this notification is provided to individuals. If applicable, outline the circumstances where the Service User will not be told about the information sharing. If the consent is due to last for a lengthy period of time, detail at what points/how often an individual will be reminded of the fair processing information and given a subsequent chance to "opt out" having previously given consent.

9 How and when might I share information?

- (A) Detail the role/name of persons sending or receiving data
- (B) Detail the name of the organisation sending or receiving the information
- (C) Detail the method of transfer – e.g. secure email, Secure FTP etc.
- (D) Detail the frequency of the transfer

10 How will shared information be recorded and held?

- (A) Name of organisation
- (B) How/Where will the information be stored by the receiving partner? Describe the physical and technical security arrangements each agency has in place?
- (C) Detail how long the information is being kept for. Do any operational retention periods apply? Can it be securely deleted once processed or do you need to keep it for a certain period of time after the transfer? The nature of the information to be shared will have a bearing on how long it should be held. Refer to your organisations record retention schedule for further guidance or discuss with the organisation(s) that is going to be providing the information.
- (D) Personal information must be securely disposed of in line with the requirement under the 7th Data Protection Principle. Describe how each agency will ensure that the personal data is

securely removed from their systems and any printed copies securely destroyed at the end of the work for which it was intended, or on termination of the contract. For example - In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste.

11 Who else can access this information?

Access should be limited to a need to know basis, specify if any internal or external parties have access to the information. For internal staff specify any vetting arrangements in place.

12 Handling Breaches

- (A) Detail the specific point of contact details for reporting any data breaches or near misses under this agreement. Where possible detail a 2nd point of contact for Business Continuity purposes.
- (B) Detail the agreed timeframes that data breaches are to be reported. As soon as possible or no longer than 24 hours after the incident was identified.

Refer to Appendix E – Handling Breaches of the Wolverhampton Overarching Information Sharing Agreement for further information around handling breaches.

13 Other measures or considerations

Add in any other measures and considerations that you may need to document within this agreement. **Example text could be:**

- Information provided by the partner will be held securely, will not be transferred to a third party, and will be used only by appropriate staff for the purposes identified.
- Electronic copies of information will only ever be held on encrypted devices or servers, will not be e-mailed outside the receiving organisation, and if transferred onto portable devices (which must be encrypted), will be disposed of securely and permanently.
- The partner organisation will not keep the personal data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the services under this agreement. Where this is necessary, the partner organisation will keep an audit trail of which laptops/drives/devices the personal data are held on.
- Paper copies of information, and printouts of electronic information, will be held securely, transferred either by safe haven fax or couriered in sealed containers and shredded upon disposal.
- Personal identifiable data will only be provided where there is a need to have that level of detail, and it is within the scope of consent on use of information given by the individual.

- The partner organisation shall employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to comply with either the NHS Information Governance Toolkit to level 2, or the requirements of ISO/IEC 27001:2005 (ISO/IEC 17799:2005) as appropriate to the services being provided.
- The partner organisation shall ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data.
- The partner organisation shall ensure that all employees used by it to provide the services as defined in the Agreement have undergone training in the law of data protection, their duty of confidentiality under contract, and in the care and handling of Personal Data;
- The partner organisation agrees to assist the Data Owner promptly with all subject information requests which may be received from the data subjects of the Personal Data;
- The partner organisation shall not use the Personal Data for any purposes other than those formally agreed with the Data Owner.
- The partner organisation shall not disclose the Personal Data to a third party in any circumstances other than at the specific written approval of the Data Owner.
- The partner organisation is NOT permitted to sub-contract any of the processing, nor transfer the personal data to any third party, without explicit written agreement from the Data Owner.
- The partner organisation will NOT transfer the Personal Data to any other country without explicit written agreement from the Data Owner.
- The partner organisation will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed at the end of the work for which it was intended, or on termination of the contract. In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste.
- The partner organisation will indemnify the Data Owner against any costs, expense, including legal expenses, damages, loss, liabilities, demands, claims, actions or proceedings which the Data owner may incur as a result of any breach of this Agreement by the partner organisation.
- This protocol is an integral part of any data sharing Agreement between the signatories to the protocol and shall be governed by and interpreted in accordance with the laws of the United Kingdom.

14 Review of this agreement

When will this agreement be reviewed to assess its validity in future? (it is recommended that each agreement is review every 12 months). Who will undertake the review?

Insert text here

Safeguarding Children in Wolverhampton – Seeking and Recording Consent

Key principles for Consent and Information Sharing

- In every case we are committed to gaining the informed consent of children and/or parents when we wish to share confidential/personal information unless in doing so it places a child at risk of significant harm or further risk of significant harm.
- We will respect the wishes of those who do not give consent, except where safety may be at risk or when it is inappropriate to seek their agreement.
- In each case of information sharing, we will record the: necessity; proportionality; and relevance of the information shared. We will take reasonable steps to obtain consent, and if it is not given, we will record why we believe safety may be at risk, or why it was inappropriate to seek their agreement. Shared information will not be kept for longer than is necessary.

1.0 Purpose

- 1.1 This guidance has been written to support Wolverhampton's partnership working to safeguard and promote the welfare of children. It specifically relates to the expectations for gaining consent and aims to provide clarity on issues relating to gaining the consent of children and families when we need to seek and share information. It also details the consent process within the Multi-Agency Safeguarding Hub.

2.0 Introduction

- 2.1 Anyone who believes a child or family requires help, has a responsibility for identifying concerns, sharing information and taking prompt action.
- 2.2 Decisions about how much information to share, with whom and when, has a profound impact on outcomes for individuals. It ensures that an individual receives the right type/level of service at the right time and may prevent their needs from escalating.
- 2.3 Poor information sharing is repeatedly highlighted in Serious Case Reviews carried out following the death of, or serious injury to, a child. Concerns about sharing information should never stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect i.e. where there is reasonable cause to suspect that a child is at risk of significant harm it is defensible to seek and share information without consent. However, it is good practice to seek consent in all cases unless in doing so would place a child at further potential risk of harm
- 2.4 Children and families have a right to privacy unless there is reasonable cause to suspect that a child is at risk of significant harm. Consent should always be sought when we want to share their information, complete assessments, or work with them. By taking reasonable steps to secure consent, professionals can maintain the trust of children and families, and ensure the best prospect of effective assessments and interventions.

3.0 Definitions

<p>Children and Parents</p>	<p>A child is generally defined as anyone who has not yet reached their 18th Birthday.</p> <p>‘Parents’ mean people with parental responsibility and other people who care for or look after children or young people. This might include other family members or adults who live in the same household.</p>
<p>Informed Consent</p>	<p>Open and honest about:</p> <ul style="list-style-type: none"> i) why we want to share information; ii) the type of information we wish to share; iii) how we would share it; and iv) who we intend sharing it with.
<p>Confidential/Personal Information</p>	<p>Confidential Information means information in whatever form relating to a Partner Agency or to a person (whether living or deceased), which:</p> <ul style="list-style-type: none"> • Is not in the public domain; • Has the necessary quality of confidence; and • Was imparted in circumstances giving rise to a duty of confidence. <p>It includes, without limitation, information in written, oral, visual or electronic form or on any magnetic disc or memory wherever located.</p> <p>It includes in particular (by way of illustration only and without limitation) information relating to the physical or mental health of an individual, whether or not such information (if in anything other than oral form) is marked confidential.</p> <p>It includes any complete or partial copy of the information.</p> <p>Personal Data – is data which relate to a living individual who can be identified:</p> <ul style="list-style-type: none"> • From those data; or • From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. <p>Sensitive Personal Data – The Data Protection Act defines sensitive Personal Data as information about:</p> <ul style="list-style-type: none"> • The racial or ethnic origin of the data subject; • Their political opinions; • Their religious beliefs or other beliefs of a similar nature;

	<ul style="list-style-type: none"> • Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); • Their physical or mental health or condition; • Their sexual life; • Their commission or alleged commission by them of any offence; or • Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.
<p>Safety May be At Risk</p>	<p>Base your decisions on considerations of <i>safety and well-being</i> of the child.</p> <p>Relevant considerations of development, care and family circumstances are contained within the <i>Additional Support</i> and <i>Intensive Support</i> sections of <i>Thresholds of Support to Children and Families in Wolverhampton</i></p>
<p>Serious risks to their health or welfare</p> <p>(s17 Childrens Act 1989)</p>	<p>Base your decisions on considerations of safety and well-being of the child.</p> <p>Relevant considerations of development, care and family circumstances are contained within <i>Intensive Support</i> section of the <i>Thresholds of Support to Children and Families in Wolverhampton</i></p>
<p>Risk of Significant Harm</p> <p>(s47 Children’s Act 1989)</p>	<p>Base your decisions on considerations of safety and well-being of the child.</p> <p>Relevant considerations of development, care and family circumstances are contained within the <i>Specialist Support</i> section of <i>Thresholds of Support to Children and Families in Wolverhampton</i></p>
<p>Inappropriate to seek their agreement</p>	<p>You should ask for consent before sharing confidential, personal and sensitive information unless there is a compelling reason for not doing so.</p> <p>For example, because:</p> <ul style="list-style-type: none"> • delay in sharing relevant information with an appropriate person or authority would increase the risk of harm to the child or young person; • asking for consent may increase the risk of harm to the child, young person, you or anyone else.

5.0 Recording decisions and actions relating to Consent

5.1 Section 6 provides guidance re. single agency recording of consent and the process within the MASH when a referral is received.

For more advice and guidance on information sharing please refer to: [Government Guidance on information sharing for practitioners](#)

6. Process for recording seeking and recording consent and progressing safeguarding referrals

Single Agency Responsibilities	<ul style="list-style-type: none">• The professional working with the family should make them aware of their intention to make a referral to Children’s Services and seek their consent.• If consent has not been given, record this in your own agency case notes and record why information is being shared without consent, include this on the Multi-Agency Referral Form (MARF).• If consent has been given, record in your own agency case notes that consent has been given and include this on the MARF.• Record in your own agency case notes the Information level you have shared and with whom.• Record on your own agency case notes that the Multi-Agency Safeguarding Hub (MASH) has been contacted for advice or to make a referral and the outcomes or actions resulting from this contact.• Record in your own agency case notes the MASH outcome and advice, how they will be completed and who is responsible.
Multi-Agency Safeguarding Hub	<ul style="list-style-type: none">• Following receipt of a MARF, the screening officers will check to ascertain if consent is required for any further action.• Where consent has not been provided and the referral is clearly for Early Help or Child in Need, then the referring agency will be contacted to obtain consent.• Where consent has not been provided but there is enough information recorded on the MARF to make an indicative assessment that there is reasonable cause to suspect that a child is at risk of significant harm then consent is not required to carry out the further checks and to progress the referral. The reason for dispensing with consent should be clearly recorded, by a manager, on Guardian.• Once a MARF has been received, the following process applies:<ul style="list-style-type: none">○ No Consent - If consent has not been provided and the nature of the request is non-urgent, the Screening Officer will contact the referring agency and provide advice and information regarding obtaining consent. The Administrator will send a standard letter to the referrer within two hours stating that the MARF has been rejected and advise that

the agency will need to re-submit the MARF once consent has been obtained.

- Within 48 hours, the administrative team will chase up progress on outstanding MARFs. This will involve contacting the referrer to enquire why a MARF with consent has not been resubmitted and to provide information, advice and guidance if required.

- **Consent provided** - If consent has been provided, the Administrative team will send the standard confirmation letter to the parent and referrer informing them of receipt of the MARF form.

Recording Process within the MASH:

- Record all contacts, including if consent has been given by the family to share information.
- Record the outcome/advice of the contact.

● **Outcomes:**

- Record and forward the contact details as part of a service referral.
- Record and forward the contact details to Early Help, consent from the family is required for action to progress.
- Record and forward the contact details to MASH, consent from the family is advised for MASH unless it is inappropriate to do so and this must be recorded.
- Undertake Level 1 Information Sharing, when appropriate, record why this is undertaken and what information has been shared & with whom.
- Undertake Level 2 Information Sharing, when appropriate, record why this is undertaken and what information has been shared & with whom.
- MASH will hold a professional or strategy discussion and record the outcome and actions to be undertaken as a result.
- MASH will process the case on the system to the appropriate agency or team.



INSERT LOGOS OF AGENCIES

Information Community Agreement

Between signatory agencies involved in the delivery of services for

Wolverhampton Multi Agency Safeguarding Hub (MASH)

Children & Young People & Adults - Information Sharing Purposes & Legal Framework

Document Control

Version	Date Modified	Author/Modified by	Summary of change
1.0	October/November 2015	Anna Zollino-Biscotti/Iain Harrison	Draft written for circulation to Workstream
1.1	23 November 2015	Anna Zollino-Biscotti/Iain Harrison & Partner Agency IG leads	Drafted edited with partner amendments
1.2	26 November 2015	Anna Zollino-Biscotti	Edited following further comments and documentation received.
1.3	4 December 2015	Anna Zollino-Biscotti	Edited following further comments received (post Strategic Board Mtg.)
1.4	16 December 2015	Anna Zollino-Biscotti	Edited following further comments from EB
1.5	30 May 2016	Iain Harrison/Anna Zollino-Biscotti	Edited to reflect Adults inclusion
1.6	22 August 2016	Iain Harrison/Anna Zollino-Biscotti	Edited with amendments from partner agency Information Governance Leads
1.7	23 August 2016	Iain Harrison/Anna	Version for signoff from Partner

		Zollino-Biscotti	agencies.

With Thanks to:

Buckinghamshire County Council
Camden Borough Council
City of Coventry Council
Devon County Council
Milton Keynes Council

[NOT PROTECTIVELY MARKED]

CONTENTS

	Page
1.0 Introduction	2
2.0 Background	2
3.0 Specific Purposes of Information Sharing under this ICA	4
4.0 Information Sharing Duties & Obligations	4
5.0 Information Types	14
6.0 Information Exchange	14
7.0 Information Security	18
8.0 Physical Security	20
9.0 Telephony	20
10.0 Clear Desks	20
11.0 Information Storage, retention & disposal	21
12.0 Movement of Information	22
13.0 Business Continuity	23
14.0 Breaches of this agreement	23
15.0 Complaints	23
16.0 Monitoring and Review	24
17.0 Indemnity	24
18 Agreement	25
18 Master Signatory Sheet	26
Appendix A	Key Statutory Provisions
Appendix B	Information Sharing
Appendix C	Multi Agency Referral Form
Appendix D	Information Governance Leads
Appendix E	Childrens MASH Process Map
Appendix F	Adults MASH Process Map

1. Introduction

This Information Community Agreement (ICA) is an agreement between all agencies working together under the remit of Wolverhampton Multi Agency Safeguarding Hub (MASH) to ensure appropriate communication and information about vulnerable children and adults is available and accessible in once place for relevant partner agencies to agree and make timely decisions.

This agreement aims to facilitate the lawful and secure sharing of information between partner agencies and designated professionals working within the Wolverhampton MASH and is a tier-2 agreement under the Wolverhampton 3-tier Information Sharing Framework.

1.1. Links to other Information Sharing Protocols:

Agreement Title	Date & Version	Lead Agency	Point of Contact
Wolverhampton Overarching ISP	Nov 2015 – V1.9	City of Wolverhampton Council	Anna Zollino-Biscotti (CoWc) Raz Bassi - RWT

2. Background

The introduction of the Multi Agency Safeguarding Hub (MASH) concept was designed to streamline the routes for referral and notifications of concern into a Local Authority and supports recommendations made in numerous Serious Case Reviews, associated academic literature and by Lord Laming within his report 'The Protection of Children in England: A progress report' (HMSO, March 2009).

The model creates a secure environment where safeguarding partners share information in a dynamic way in order to identify and assess risk which in turn ensures social care decision makers are able to make necessary and proportionate decisions based on the best possible information available at a given time.

The original MASH concept for safeguarding and promoting the welfare of children was designed to:

Provide the highest level of knowledge and analysis of all known intelligence and information across the safeguarding partnership to ensure all safeguarding activity and intervention is timely, proportionate and necessary.

The MASH acts as the first point of contact for receiving safeguarding concerns about vulnerable people and provides an immediate opportunity to collate information from different agencies in order to build up a holistic picture of the circumstances of each case.

This allows the MASH to:

- Undertake information based risk assessments and decision making to identify those young people who require support or necessary and proportionate intervention.
- Victim identification and harm reduction to ensure partners work together to deliver harm reduction strategies and interventions for both victims and those who are likely to experience harm.
- Co-ordinate partner safeguarding by signposting the needs of vulnerable young people and adults to the relevant partner(s) to ensure harm reduction strategies and interventions are delivered.

The MASH helps to ensure appropriate communication and information is available and accessible in one place for relevant partners to agree and make timely decisions.

The MASH does not replace established child or adult safeguarding procedures for investigation and remedy. The MASH collates information from all available sources in order for the most informed decision to be made concerning any required intervention. All interventions are required to be necessary and proportionate.

Through bringing key professionals together to facilitate early, better quality information sharing, analysis and decision making, the MASH enables the 'system' to safeguard vulnerable people more effectively. Having representatives from agencies such as the police, health, education and social care in one office ensures that key professionals are appraised of all available information before making safeguarding decisions. Information from different agencies is collated and analysed and used to inform the action that needs to be taken, resulting in people being protected and receiving the support that they need more quickly.

Evidence shows that sharing information is vital to better safeguard and promote the welfare of children and adults with care and support needs. Information sharing is also one of the main areas where improvements have to be made in the review process. The MASH makes information sharing easier by:

- Providing all professionals with more information to make better decisions (and is legally compliant)
- Being a confidential environment so all material (sensitive or not) can be revealed to each agency to decide what action should be taken

While all the models across the region and country are slightly different, the increase in information sharing and a fully integrated system for shared decision making ensures improved quality of decisions and a more timely process for better protecting children and vulnerable adults.

The aim of this agreement is to define how personal and sensitive personal data, as defined by the Data Protection Act 1998, will be securely and lawfully shared between the partners.

3. Specific Purposes of Information Sharing under this ICA

As part of Wolverhampton MASH operating procedures, agencies are asked to disclose, receive and retain personal, sensitive information. This ICA describes the purposes for which information will be used under the remit of the **Wolverhampton MASH** in order to promote the appropriate communication and exchange of information between all agencies working together to safeguard and support the wellbeing of children and adults in Wolverhampton.

All agencies under this agreement will be bound by legislation, guidance and common law which will determine their ability to disclose, receive and process information.

As a minimum, to ensure effective safeguarding arrangements, this agreement will:

- outline the principle for sharing information between agencies, professionals and other statutory bodies;
- outline the principle and standards of expected conduct and practice of partner agencies and staff working for them; and
- provide a framework for the legal, secure and confidential sharing of information between agencies and professionals.

It is important to note that information sharing on a case to case basis between professionals should not depend on the existence of an agreement being in place between the relevant agencies. **The absence of a protocol should not prohibit the sharing of information.**

4. Information Sharing Duties & Obligations

There is no single source of law that regulates the powers that an organisation has to use and to share personal information. Sharing information between agencies is lawful if:

- Consent is given; or
- The public interest in sharing the information outweighs the obligation of confidentiality owed to the individual such as safeguarding a child or vulnerable adult's welfare or (this would be on an individual case by case basis and not the sharing of large volumes of data);
- Disclosure is required under a statutory obligation e.g. to support investigations made under Section 47 of Children Act 1989 or Section 42 of the Care Act 2014

In order to share information legally between partners there must be a defined and justifiable purpose that references the appropriate underpinning legislation and the associated duties and/or powers.

It is therefore the responsibility of all signatories to this agreement to ensure that any information exchanges are justified and in adherence with the following:

- The law that governs the actions of public bodies (administrative law) – each agency needs to establish whether they have the power to carry out the function to which the data sharing relates.

Further details of statutory powers and gateways are provided at **Appendix A**.

4.1. The Data Protection Act 1998 – each agency must ensure that information being shared is done so in line with the principles of this Act, and in particular the sharing of information meets the conditions for the processing of personal data (schedule 2) and the processing of sensitive personal data (schedule 3).

Each partner to this agreement is the Data Controller for their organisation's information and is solely responsible for securing their lawful basis for sharing.

Personal data processed within the MASH regarding outcomes becomes the responsibility of the MASH/Council as data controller and MASH owner. Each individual agency is the data controller for the information that is held in their individual systems. Each agency responsible for the information they input into the MASH/Guardian system will be data controllers in common in respect of their control over what information is processed within the system.

The 8 principles of the Data Protection Act 1998 have been used to provide a framework within which to consider the lawful basis for sharing information under this agreement.

4.1.1. 1st Principle

Personal data must be processed fairly and lawfully.

This means, that for a partner to share personal data it must have some legal power for doing so. It should be emphasised that Section 29 of the Data Protection Act 1998 does not give a direct power to disclose information, it does however state 'that if not disclosing information would prejudice the prevention/detection of crime and/or the apprehension/ prosecution of offenders, personal data can be disclosed'.

Section 29 of the Data Protection Act 1998 allows agencies to share information if complying with the fair processing conditions i.e. telling individuals how their data will be processed/shared; would be likely to prejudice the purposes of the prevention or detection of crime and or the apprehension and prosecution of offenders.

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

Sharing information about concerns regarding young people will often fall below the statutory threshold of Sections 47 or 17 of the Children Act 1989 or equivalent provisions contained in the Care Act 2014 in regard to vulnerable

adults. This does not mean however that such issues are ignored. It may be appropriate (and lawful) to direct individuals at potential risk to either Childrens Early Help or Adults Local Teams for assistance.

If concerns do however fall within these sections of the 1989 or 2014 Acts, then these sections will be the main legal gateway for sharing the information.

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

Sections 1-7 of the Care Act 2014 also place obligations on local authorities to co-operate with partner organisations and promote well-being and also integrate care and health services to prevent the need for care and support arising.

In addition Section 42 of the Care Act 2014 gives three criteria that must be met to trigger an enquiry (investigation) by a local authority. These are:

- An individual has care and support needs; and
- Is experiencing or is at risk of abuse and neglect; and
- Is unable to protect themselves.

Where engaged, these provisions create a “permissive gateway” for information to be shared in a lawful manner.

Such information sharing must take place in accordance with statutory requirements of the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

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

All decisions to share or not share information must be decided on a case-by-case basis and recorded in the MASH system (Guardian).

Duty of Confidence

Partner organisations recognise the importance of the legal duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are lawful grounds and an overriding justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

A Duty of Confidence may be owed to both the holder of the data and to the data subject.

All health data is subject to a 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 police will act appropriately with regards to the information for the purposes of preventing harm or promoting the welfare of children.

Whilst always applying the tests of proportionality and necessity to the decision to share information, the protection of children or other vulnerable persons would clearly fulfill a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim. All information shared with a partner agency must be relevant to the case in point.

Information held by other agencies that will be shared in the MASH may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure, as information can be shared where consent has been provided or where there is a strong enough public interest to do so. Partners will have the ability to restrict access to certain personal data being shared.

Consent

Obtaining consent remains a matter of good practice, and where circumstances allow, consent should be informed (explicit). Practitioners, where possible and appropriate, should encourage clients to view the sharing of information – and their consent to share their information - as a positive and beneficial step that facilitates the provision of services that they require. Consent will be recorded within the relevant system at the point it is referred to the MASH Triage.

The starting point in relation to sharing information is that practitioners will be open and honest with families and individuals from the outset about why, what, how and with whom information will or could be shared with. The City of Wolverhampton Council's Privacy Notice provides this, as does the Wolverhampton MASH privacy notice.

There will be no breach of confidence where consent has been provided by the person who a duty of confidence is owed; consent can be **explicit** (verbal or in writing) or can be **implicit**, whereby consent is implied from the discussion or circumstance where the information was provided. Implied consent should not be relied upon when the information is of a very sensitive-personal nature; explicit consent (preferably written) should be obtained in these situations.

Where a person does not have the capacity to give consent to share their information, consent should be sought from someone who is in a position to appropriately act on their behalf, e.g. an appropriate adult or someone who holds a relevant power of attorney. If this is not an option an appropriate professional should make a best interests decision.

There may be occasions when it is judged that a refusal of consent would put a child/young person or others at risk of significant harm, or an adult at risk of serious harm or would undermine the prevention, detection or prosecution of a

serious crime. In these circumstances, there is an expectation that the refusal of consent would be overridden and that information would be shared. Where consent has not been provided, this will be recorded also, along with reasons why the information is being shared for referral into the MASH.

There must be a proportionate reason for not seeking consent and the person making this decision must try to weigh up the important legal duty to seek consent and the damage that might be caused by the proposed information sharing on the one hand and balance that against whether any, and if so what type and amount of harm might be caused (or not prevented) by seeking consent.

In general consent should not be sought when information sharing is required by law, through a statutory duty or court order, or in circumstances that would:

- place a child or young person at increased risk of significant harm; or
- place an adult at risk of serious harm; or
- prejudice the prevention or detection of serious crime; or
- lead to an unjustified delay in making enquiries about allegations of significant harm to a child or serious harm to an adult

There is no absolute requirement for agencies in the MASH to obtain consent before sharing information nor is there a blanket policy for never doing so.

Members of the MASH will, however, consider on all occasions and on a case by case basis whether information will be shared with or without consent.

This determination by a practitioner should always be reasonable, necessary and proportionate. It should always be recorded together with the rationale for not seeking consent, which must be electronically recorded to provide an audit trail.

Privacy Notice

A requirement of the Data Protection Act 1989 is that all organisations that process personal data should have what is known as a "Privacy Notice" which will inform individuals about how their personal data will be used by that organisation. This notice will cover:

- The identity of the data controller
- If the data controller has nominated a representative for the purposes of the Act, the identity of that representative
- The purpose, or purposes, for which the data are intended to be processed
- 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

City of Wolverhampton Council will publish a Privacy Notice specifically relating to the Wolverhampton MASH and partner organisations will link to this and all publish a Privacy Notice in their normal manner.

The Privacy notice can also be accessed from the Wolverhampton Adults Safeguarding Board:

[Wolverhampton Safeguarding](#)

Legitimate Expectation

The sharing of the information by police fulfils a policing purpose, in that it will be done in order to protect life in some circumstances and in others it will fulfil a duty upon the police provided by statute law (Children Act 2004 and the Care Act 2014) i.e. co-operation to safeguard or promote the well-being of children and vulnerable adults

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

Consent will have been considered before the individual's case is brought to the MASH. If consent has not been sought/gained, the reasons why will be documented.

In cases, where consent has been granted individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why.

Human Rights Act 1998 – Article 8

The Right to Respect for Private and Family Life, Home and Correspondence:

“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Consent is relevant to the rights of those to whom confidential information relates. Article 8 is a 'qualified right' and there will be no contravention of sharing information without consent provided the sharing with children's or adults services is necessary in a democratic society, is in accordance with the law and is necessary for the prevention and detection of crime, for the protection of health or morals, or for the protection of rights and freedoms of others.

The benefits of 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.

The promotion of the welfare and wellbeing of children and ensuring they achieve all five outcomes is, by virtue of Section 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

An activity appropriate and necessary in a democratic society:

The police are obliged to do all that is reasonable to ensure the welfare of the most vulnerable of citizens and this is something that is necessary and appropriate in a democratic society.

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

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

Schedule 2 of the Data Protection Act 1998

In addition to the legal criteria set out above, the information sharing arrangements 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 Section 10 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". Similar provisions exist under Section 45 of the Care Act 2014.

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

Schedule 2 of the Data Protection Act 1998

If the information is "sensitive" (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of

any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3.

Schedule 3 is satisfied in the case of this agreement by condition 7, 'the processing is necessary for the exercise of any functions conferred on any person by or under an enactment' i.e. as mentioned above, Children Act 2004. Or the Care Act 2014.

Where the explicit consent (in writing or otherwise expressed and recorded) of the individuals involved is received, Condition 1 of Schedule 3 (data subject has given explicit consent to the processing of their data) will apply.

4.1.2. 2nd 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.

Under this arrangement Personal data will not be processed in any manner contradictory to purposes for which it was collected.

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

4.1.3. 3rd Principle

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

It is the responsibility of each partner agency to this agreement to determine what information their agency will disclose and to which partner(s) of the MASH.

Due to the complexity of the MASH, providing a prescriptive list of data fields to be shared is difficult. Any information that is shared into, within or out of the MASH Hub will be decided on a case-by-case basis and must be relevant to the aims of this agreement and the rationale electronically recorded.

4.1.4. 4th Principle

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

All the information supplied will be provided by partners either from their computer systems or from a paper record and as such will be subject to their own organisations reviews, procedures and validation.

Any perceived inaccuracies should be reported to the contact at that agency for verification and any necessary action.

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

Specifically this means that the data fields exclusively relate to individual actions or events that will have already occurred at the time of sharing. These are not categories of information that will substantially alter or require updating in the future.

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

Where new information is being referred into the Triage or MASH via the Multi Agency Referral Form (MARF) for children or SA1 forms for adults the accuracy of the information is the responsibility of the professional who has provided it; likewise where information has been keyed into the MASH system (Guardian), responsibility will sit with the MASH professional who has updated the system.

4.1.5. 5th Principle

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

Individual agencies will retain their information in line with the individual organisation's disposal 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.

Information that is shared into the MASH will already be covered by the providing agency's retention and disposal schedule, therefore the retention of information by the MASH will be for no more than 5 years after it has completed its referral responsibilities.

4.1.6. 6th Principle

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

No direct marketing to those being safeguarded will be undertaken. Any requests received that relate to information being processed under the Wolverhampton MASH should be directed to the City of Wolverhampton's Information Governance Team in the first instance.

Partners will be responsible for the processing of requests regarding their own employees and data subjects, liaising with the MASH manager as required.

The City of Wolverhampton Council and partners to this arrangement will respond to any notices from the Information Commissioner that imposes requirements to cease or change the way in which data is processed and will comply with subject access requests in compliance with the relevant legislation.

See **Section 4.3.1** of this document for further information relating to Subject Access Requests.

4.1.7. 7th 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 this principle are outlined in **Section 7** of this document.

4.1.8. 8th 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.

Information input to the MASH system (OLM Guardian) is held in a Cloud based service with a dedicated server & rack, locked cage firewall with access only for MASH and hosted in an ISO 27001-certified UK data centre.

For Adults safeguarding, Police and Health agencies will have a “virtual” presence in the MASH, accessing OLM Guardian via a secure link.

Under the terms of this agreement no information will be passed outside of the European Economic Area unless a 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.

4.2. Legal Considerations

A more detailed list of relevant legal considerations relating to information sharing is provided at **Appendix A**. This section also contains a table of specific considerations that support the legal gateway

In addition, the following documents provide additional useful information and are considered an accurate summary of the legal principles and what the law requires for decision making to be lawful in relation to the sharing of information.

- Centre of Excellence for Information Sharing (multi-agency safeguarding hubs)
- Information Sharing – Advice for practitioners providing safeguarding services to children, young people, parents and carers.
- ICO Data Sharing Code of Practice
- HM Government Information Sharing Guidance for practitioners and managers
- HM Government Information Sharing Guidance on legal issues
- The West Midlands Joint Protocol for Child Protection & Related Criminal Investigations

4.3 Data Protection Requests and Freedom of Information Requests

4.3.1 Data Protection Requests

This agreement supports the rights of a data subject, as outlined in Section 7 of the Data Protection Act 1998. This agreement also covers request received under other sections of the Data Protection Act 1998.

The City of Wolverhampton Council's Information Governance team will process all Data Protection requests received directly for the MASH.

In the unlikely event of a partner agency receiving a request for information processed by the MASH, they should send it to the City of Wolverhampton Council's Information Governance Team at:

Information.governance@wolverhampton.gcsx.gov.uk

The team will then allocate and process the request via the MASH Manager, who will ensure the relevant partner agency is consulted when the information being sought falls under their responsibility as Data Controller.

All partners to this agreement will provide a list of contacts to deal with queries and requests for information under the Data Protection Act 1998 from the MASH.

4.3.1 Freedom of Information Requests

City of Wolverhampton Council Information Governance team will process all freedom of information requests received directly for the MASH.

This document and the arrangements it details will be disclosed for the purpose of the Freedom of Information Act 2000 and will be published within the signatories' Publication Schemes.

A partner who receives an access to information request that relates to their organisation's data, will process it via their relevant internal procedures. Prior to a partner organisation responding to an information request involving data belonging to another partner, they will consult with the relevant organisation and consider their views in the decision making process.

All partners to this agreement will provide a list of contacts (**Appendix D**) to deal with queries and requests for information under the Freedom of Information 2000 from the MASH.

5. Information Types

There are various types of information that agencies subject to this agreement may manage and share:

Person-identifiable information: This is information that enables an individual to be identified, such as a service user, patient, client or employee. This information can also be confidential and/or **sensitive** in nature and therefore needs to be handled with greater care and consideration.

Organisational information: This being plans, policies, guidelines and minutes of meetings. This is information that is generally freely available under the requirements of the Freedom of Information Act, subject to specific exemptions.

Statistical information: This is aggregated or anonymised information that is statistical in nature and usually shared between agencies. This kind of information is structured to avoid the identification of individuals.

Anonymised information: This is data which has had identifiers removed so that an individual cannot be identified.

Pseudonymised information: This is data which has had identifiers removed and replaced with a pseudonym.

6. Information Exchange

6.1. General Principles:

All information exchanged under this agreement must be:

- Relevant to all necessary actions and procedures applicable to the Wolverhampton MASH and
- Be shared for the specified purpose; and
- Be shared in circumstances justifying the need to share information.

This ICA draws heavily on the HM Government “Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (March 2015) and HMG “Information Sharing: Guidance for practitioners and managers” published in 2006 by the Department for Education and Skills. All agencies signing up to this agreement must have regard to this guidance as detailed in **Appendix B**.

6.2. Non-Routine Personal Sensitive /Confidential Information

This type of information will be the bulk of information shared for the purposes of the Wolverhampton MASH.

This type of information cannot be shared without the prior explicit consent of the client/data subject, unless an overriding statutory obligation or public interest in disclosing the information outweighs the duty of confidence owed to an individual e.g. safeguarding a child’s welfare.

Section 4 of this document covers the statutory duty to share information for the purposes of the Wolverhampton MASH.

Section 6.5 of this document outlines the process followed when sharing information.

6.3. Routine Personal Sensitive Information sharing

Should routine sharing of specific personal and personal sensitive information be required between agencies, it is recommended that a Purpose Specific Information Sharing Agreement is completed (Tier 3 PSISA) to ensure that the specific requirements for sharing information are documented and agreed. A tier-3 PSISA template can be found in Appendix F of the Wolverhampton Overarching Information Sharing Protocol.

6.4. Routine (Anonymised/statistical) information

Signatories of this agreement agree to share aggregated and statistical information to plan and monitor progress of a particular service under the remit of The Wolverhampton MASH provided the information does not identify individuals and cannot re-identify individuals when pieced together with other information. Each agency should ensure that the appropriate risk-identification assessments have been carried out (such as motivated intrusion test) to eliminate the risk of re-identification, prior to providing such information. The NHS number will be used as the common identifier for this purpose and pseudonymisation techniques will be implemented. Where health information is being used for risk stratification purposes, the appropriate risk stratification procedures should be followed.

Aggregate and management information of this type can be shared without client consent.

6.5. Format of information disclosure/exchange

6.5.1 When the MASH receives a referral, the MASH Screening Officers first check if the child or adult is already known to a City of Wolverhampton Service e.g. Adult Social Care, Childrens Early Help and Youth Offending.

If it is an open case, or a case that has been closed within the last 28 days, the allocated worker is considered to be the best person to support the individual, so the case is referred directly to them.

If there is no allocated worker, then the MASH social workers will collate any relevant information, which may include, accessing other systems such as Housing information and present this to the Lead Professional for Social Care Early Help and Adults within the MASH. The Lead Professionals for Social Care & Early Help will then review the information and apply a threshold/RAG.

The Consultant Social Worker may change the RAG rating as new information comes to light. Similarly, where referrals have gone direct to Children's Early Help or a local Adults team, if more information is received that indicates the risk may be higher, this will be stepped back up to the MASH to reassess the threshold

Where personal sensitive information is being discussed/ disclosed in a multi-agency forum (case conference, professionals meeting etc.), the following guidelines should be followed:

- All those in attendance of the meeting/forum should sign a meeting attendance form. Any person in attendance, who does not represent an agency signatory to

this agreement, should be asked to sign a confidentiality agreement.

- The grounds for disclosure should be recorded and these should be minuted and stored securely with the minutes of the meeting.
- The minutes of the meeting should be securely distributed and stored in accordance with the guidance issued in this document - Section 7.0, 8.0 & 11.0 or local policies and procedures.

6.5.2 All referrals into the MASH made by professionals or participating agencies, should be made in writing unless the matter is urgent, in which case the request or reply should be followed up in writing. Where appropriate, requests should be made using the **Multi-Agency Referral Form** (MARF or SA1) provided in **Appendix C**.

- Requests for information should be responded to by the agency holding the information within an agreed number of days. The following thresholds will apply:
 - **RED** - There is a potential child or adult protection issue (e.g. serious injury to the child or an immediate risk of harm or neglect to an adult). To be dealt with in 4 hours (or immediate if required) – straight to Strategy or Planning Discussion. In some cases information will still be collated from agencies within the MASH to inform future decisions/plans. If the final RAG rating is Red, the case will be investigated by the MASH safeguarding team
 - **AMBER** – There are significant concerns but immediate action is not required. For example, safeguarding criteria under Section 42, Care Act 2014 are not met. Cases to be dealt with in 24 hours for Childrens/1 working day for adults. – Referred into MASH for information gathering and a MASH planning discussion to inform ation. If the final RAG rating is Amber, the case will be either investigated by the appropriate local adult social care team or the MASH safeguarding team.
 - **GREEN** - There are concerns regarding a child or adult's wellbeing but these do not meet statutory requirements (e.g. poor school attendance or adult safeguarding criteria). To be dealt with in 72 hours for Childrens/3 working days for adults – straight to Early Help for childrens cases or local adults area teams/appropriate agency for action.

For reds and ambers the Consultant Social Worker will decide what agency information is required and then trigger an information request using the MASH Guardian System. This will include the referral information and the RAG rating that has been applied.

- The process for data input in to the Council's OLM Guardian system will allow that cases can be created just in Guardian and will generate a searchable reference field in Guardian so that if staff get a re-referral then they can find the original.
- This means that if a referral comes in and it's a child or adult not previously known to us and the family only need Early Help or local adult team input then that will be created separately on Guardian (and the Early Help system for

children) but not on CareFirst.

- If there is any uncertainty and we need to start asking for further information then at that point the child or adult will need to be created in CareFirst if not previously there.
- As soon as staff starts to create somebody in Guardian then it searches CareFirst so as to prevent duplications so if there is information in CareFirst it will automatically populate Guardian with the basic demographic details.
- If a family was previously open to social care and the referral comes in and passes to Early Help then staff can just generate an observation in Care First recording this.

Information inputted in Guardian that is purely early help or local adult team (GREEN) will not go onto the social care system and be MASHED.

Consent will be recorded on the Guardian system as per the MARF and SA1 forms.

Where consent has not been obtained as a result of the family/individual not wanting to provide it, this should be recorded (again as per the MARF and SA1). Reasons why consent may not be required will include:

- Where the practitioner believes that there are concerns that this could be a potential Child in Need or adult with care and support needs– the information can be recorded in Guardian under the provisions of Section 17 of the Children Act 1989 and Section 42 of the Care Act 2014 for adults and again, the practitioner must include why the information was shared without consent.
- Where consent is not gained and there are no concerns – then the information is inputted and not shared with anyone.

In general:

Each partner agency will already have in place documented business processes and procedures that identify and inform staff of circumstances that are adversely impacting upon the welfare or wellbeing of a young person or adult that will result in a referral to the MASH.

The MASH will have documented business processes and procedures for processing, which will identify those agencies that will be informed and take an active role in the intervention or protective measures that need to be put in place.

Such processes will include the necessity for electronic and hardcopy information to be protectively marked and a confidentiality statement for strategy/conference meetings and outputs, e.g. minutes, plans etc.

With the exception of subject access requests, any identifiable information relating to health patients will only be accessed and processed by qualified professionals (such as social workers or lead nurses) involved in the direct care of a patient.

The MASH will seek the permission of the originating agency if they wish to disseminate information outside of the MASH environment. Such permission will only be granted where the proposed sharing is within the agreed purposes for safeguarding and supporting the wellbeing of young people or for policing purposes.

Where there are lawful grounds to share person identifiable information outside of MASH, e.g. to an ad hoc partner agency who will be assisting with proactive intervention work, the MASH will ensure that it is provided securely and the receiving body is only provided with minimum level of information in order to fulfil their role.

MASH will ensure authorised recipients are informed that they must comply with the security controls within this agreement, emphasising the:

- Sensitivity of the data and requirements for confidentiality, as documented within the system (on Guardian)
- Security controls required to safeguard the data
- Protective marking
- Process for reporting any suspected or actual information security breach
- Partners to this agreement will maintain an accurate, secure record of person identifiable data that has been shared.

The process followed by the MASH is detailed at **Appendix E.** for Childrens and **Appendix F** for adults.

7. Information Security

7.1.1. All agencies signatory to this agreement acknowledge the security requirements of the Data Protection Act 1998 and ensure that the necessary technical and organisational measures (e.g. IG Toolkit Level 2, ISO 27001 or equivalent Government standard assurances as appropriate to their organisation) to safeguard and secure against unlawful processing, accidental loss or destruction or damage to personal and personal sensitive information.

7.1.2. Access to information subject to this agreement will be granted to those professionals who “need to know” to effectively discharge their duties.

7.1.3. ICT Systems:

The ICT server, switches and cabling supporting the connections to each partner’s IT infrastructure are located in a controlled secure environment that is managed through an agreed change control process.

Each agency’s MASH personnel will be able to securely connect to their organisations relevant ICT systems.

All personnel within the MASH will have individual unique user accounts to a secure web-based Council’s OLM Guardian System. This will allow authorised users to input relevant information from their organisation’s systems into the MASH module.

Personnel will not have access to any other systems that belong to other partners of the MASH.

Access permissions will only allow authorised users:

- From the individual organisation's to edit/add their organisation's information, which they can make invisible to other MASH members until it is submitted for a decision;
- To search for existing clients within the MASH module
- The MASH module will audit all user actions barring export of data from the system (which shall be manually audited)
- Only encrypted authorised laptops and/or storage devices will be used.
- All MASH personnel have a responsibility for the management and protection of ICT assets from deliberate, unintentional or unauthorised access, modification, destruction or disclosure and will take reasonable measures to reduce the risk of theft or loss.
- Desks will be positioned to reduce risks such as shoulder surfing and, where necessary, privacy screens will be attached to monitors.
- All MASH personnel will have their own secure storage area, where equipment can be locked away when not in use.

7.1.4. Information should be classified and managed in accordance with the Government Protective Marking Scheme (GPMS) where it is being sent to or received by a public sector organisation, such as the local authority, police and health.

The information to be shared under this agreement is sensitive personal data and is classified as 'OFFICIAL – RESTRICTED' under the Government Security Classifications Scheme April 2014.

Prior to April 2014 such information may have been marked PROTECT or RESTRICTED and will assume the same status as 'OFFICIAL – RESTRICTED'.

The NHS protective marking 'NHS – Confidential' assumes the same status as 'OFFICIAL – RESTRICTED'.

7.1.5. Each agency will ensure that there are appropriate arrangements in place to ensure the security of electronically transferred information:

- Personal and personal sensitive information (protected or restricted information) sent by email must be sent via a secure email system such as GCSX for public sector organisations (GCSX, PNN, GSX, CJSM, NHSnet and N3) and secure messenger (e.g. City of Wolverhampton Council secure email facility) for other agencies.
- For Adult safeguarding cases, completed SA1 forms must be sent by secure email for uploading to the Council's CareFirst system.
- All adults and children's referrals made into the MASH from a public sector

organisations (Health, Police, other Local Authorities, Probation etc.) should be sent to

MASH@wolverhampton.gov.uk

Or:

MASH@wolverhampton.gcsx.gov.uk

8. Physical Security

The MASH office will be located in a secure central office within the City of Wolverhampton Council's Civic Centre offices, separate from other areas of the business and to members of the public.

Only authorised staff (MASH personnel, authorised visitors) will have access to this area and physical access to the office will be via a restricted pass access system. All MASH and supporting personnel are required to wear identification tags/cards.

Secure storage and meeting rooms are located within the MASH office. Meetings will be undertaken in designated meeting rooms, or other appropriate location within the MASH.

During working hours, the MASH office is manned. Outside of working hours the building is alarmed and remotely monitored by the City of Wolverhampton Council.

All partner agencies will operate an effective 'starters, leavers, movers' process that ensures physical and logical access is suspended or terminated appropriately.

It is the responsibility of each agency to promptly inform the MASH Manager of any requirements to suspend/terminate physical access to the MASH offices and/or the MASH ICT system.

The MASH processes and procedures will incorporate, where applicable, requirements for managing the security and lawful use of electronic and paper records. Irrespective of whether the data is electronic or hard copy, physical and technical access to personal data will be regulated on a 'strictly need to know' basis.

All procedures should demonstrate good practice guidance has been applied.

9. Telephony

MASH will have access to dedicated phone lines for use by partner agency staff in the MASH. MASH personnel will ensure confidentiality is maintained when using desk and mobile phone equipment. This will be achieved by being aware of who may be able to overhear a conversation, not leaving personal/sensitive personal data on voice messages or sending it via SMS (and similar).

10. Clear Desk Policy

MASH personnel will operate a 'clear desk policy'. This will include:

- Locking away all Protectively Marked, sensitive and valuable documents (eg paper records, notes, removable media such as CD/DVD etc) in their allocated lockers/cabinets when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight;
- Locking workstations (computers, laptops) when unattended by pressing Ctrl Alt Delete, or similar
- At cease of work close down all the applications and log off/shutdown the workstation
- All mobile equipment, e.g. laptops, must be stored securely and not left out on desks when the user is not in attendance at the office
- If, in an emergency, partners need to leave the office quickly, e.g. a fire alarm or emergency call, invoke the password-protected screensaver, ONLY IF IT IS SAFE TO DO SO
- Ensure monitor screens are positioned to prevent protectively marked information from being read by others.
- Passwords, Building access cards (or similar) must be kept safe and not shared with others.
- Print and post trays will be regularly checked to remove sensitive documents

11. Information storage, retention and disposal.

11.1. All agencies party to this agreement will ensure that they have in place policies and procedures governing the secure storage of all personal information within their manual and electronic storage systems.

Electronic copies of information should only be held on encrypted devices or servers and should not be transferred to portable devices unless such devices are fully encrypted and their use is necessary for the provision of services under this agreement.

11.2. Storage of Information on partner's systems.

- All Partners to this agreement will input outcomes from the MASH into their own systems.
- Partners will confirm that there are adequate security measures on their electronic systems to protect information that has been provided by partners.
- Information can only be accessed via unique username and authentication controls. Partners confirm that permission to access MASH information held electronically by partners will be granted on a strict 'need to know' basis once it is contained within partners' electronic systems.

11.3. The retention of information held in manual and electronic systems

- Information processed under this agreement will only be retained for a minimum

period as necessary in relation to the purpose for which it has been provided and then securely destroyed when that period comes to an end.

- Information processed on the Guardian system will be retained for the appropriate period specified by statute or best practice after the episode has been closed.
- Information held on each agency's IT systems will be retained in accordance with the agency's retention and disposal schedule.

11.3.1. The secure disposal of electronic and manually held information within the MASH;

- The City of Wolverhampton Council will ensure that personal and personal sensitive information held on the Guardian system will be securely removed from the system and that printed documentation is securely destroyed at the end of its retention period.
- Electronic information will be securely destroyed by the physical destruction of the storage media or by the use of electronic shredding software that meets government standards or ISO 27001 to ensure permanent deletion.
- Hard copy information will be destroyed by cross-cut shredding and secure recycling of the paper waste in accordance with the City of Wolverhampton Council's confidential information disposal policy.

12. Movement of information

12.1. Post - Whilst it is unlikely that the MASH team will receive sensitive personal data via external or internal postal arrangements, there may be occasions where there is a need to send such information to an authorised recipient.

When sending post to an external authorised recipient using courier, recorded or special delivery means, the sender will ensure that the:

- Information has been protectively marked;
- that the recipient's address is accurate;
- a sealed/window envelope with a printed return address is used;
- the team's identification stamp is applied (to ensure any returned post is returned to the MASH team unopened)

12.2. Printing and scanning facilities –

Printing of hardcopy information and production of handwritten notes is discouraged but should this be required, only dedicated Council secure printer/scanner facilities, located in a secure environment, must be used.

Printed information will only be sent to a secure printer and must be immediately collected by the authorised user.

Printed information should be kept securely and securely disposed of when no longer required.

12.3. FAX - Use of Fax facilities is not encouraged and will not be available to the MASH team, other than via dedicated Multi-functional-devices (MFD) available within the MASH area.

13. Business Continuity

The MASH office is located in the Civic Centre and is accessible Monday-Friday 08.30-17.00 PM.

In the unlikely event that the MASH office cannot be physically accessed, members of the MASH will operate from their own agency's premises and, providing IT systems are still available, will continue to operate as a 'virtual team' using the secure links to the MASH module.

ICT system management arrangements will be in place to protect and support the MASH from risks that could impact the confidentiality, integrity and availability of information.

14. Breaches of this Agreement

All agencies who are party to this agreement will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

In the event of personal information that has been shared under this agreement being compromised, whether accidental or intentional, the organisation/agent making the discovery will without delay:

- Notify the MASH Manager of any actual or suspected incident that has, or is likely to result in a breach of the Data Protection Act 1998.
- The MASH Manager will address any immediate safeguarding concerns as a result of such an incident and promptly inform City of Wolverhampton Council's Information Governance Manager and the relevant partners nominated information governance leads(s) in order to ensure appropriate action is taken to contain, recover and learn.
- Depending on a number of factors, this action may also result in the relevant agency/ies implementing internal disciplinary proceedings.

Partners may also consider the need to report any actual breaches to the Information Commissioners Office (ICO)

15. Complaints regarding information shared under this agreement

Where complaints are received regarding the use of information shared under this

agreement, the City of Wolverhampton Council's Information Governance team will handle complaints received directly by the MASH, notifying relevant partner agency Information Governance Leads. If the information consists of data provided by a partner agency, the information governance lead for that agency will be immediacy informed.

In the event a partner receives such complaints, the receiving partner's Information Governance Lead who is the focus of the complaint will co-ordinate the response in consultation with the MASH Manager, The City of Wolverhampton's Information Governance Team and relevant partner agencies (if applicable).

16. Monitoring and Review of this ICA

This agreement will be reviewed by the City of Wolverhampton Council, in consultation with Partner Agencies every 12 months and changes recorded in the version control.

It is the responsibility of each agency signatory to the agreement to ensure that they have the latest version of this agreement

17. Indemnity

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. This must be documented formally and without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

Each partner will keep the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and, in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

Data controllers sharing personal data on data subjects for the purpose of the MASH will be responsible for their own or their employee's actions and will be liable for any breach they incur under the Data Protection Act 1998 and neither partner intends that the other partner shall be liable for any loss it suffers as a result of its or its employees actions.

18. Agreement

Agreement for <Enter Organisation Name>:

We accept that this Information Community Agreement will provide a framework between the signatory organisations for the secure sharing of information within the Wolverhampton MASH 'Information Community' in a manner compliant with their statutory and professional responsibilities.

Signatories undertake to:

- implement and adhere to this ICA in the context of the Wolverhampton Three-Tier Model for Information Sharing.
- ensure that all protocols and procedures established within the organisation and between the organisation and others for the sharing of information are consistent with this ICA;
- establish systems, raise awareness, inform service users, issue specific guidance, and provide training to their staff to ensure compliance with this agreement;
- ensure no restrictions will be placed on sharing information other than those specified in this Agreement, the Overarching Policy, or other relevant service-specific Information Sharing Protocols.

This agreement is signed by Enter name of Director or the equivalent functional leads of each signatory organisation, and/or the Caldicott Guardian where applicable, on behalf of their organisation.

<Name > (of Director or equivalent functional lead)	
Signature:	
Name:	
Position:	
Date:	

Caldicott Guardian (where applicable)	
Signature:	
Name:	
Position:	
Date:	

19. Master Signatory Sheet (Administration Use Only)

The following sheet is to be completed and updated by **the owner/lead agency** of this agreement following completion of the Agreement form in Section 13 by each individual agency signing up to this agreement.

Organisation	Name of Signatory (& Signature)	Designation/Role	Date Signed

Appendix A – Key Statutory Provisions

Administrative Law

Local Authorities and other public bodies derive their powers entirely from statute. These bodies must not act outside those limited statutory powers. It is a well-established principle that express statutory powers should be interpreted so as to authorise “the performance of acts reasonably incidental to those expressly granted”. This principle is reflected in section 111 of the Local Government Act 1972 that provides that local authorities are expressly empowered to do “anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions”.

There is no general statutory power to disclose data, just as there is no general power to obtain, hold or process data. As a result, it will be necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied from the terms of the legislation. Clearly, express powers to share data give the highest degree of certainty, but it should be borne in mind that such express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked.

If there are no relevant statutory restrictions it may then be possible for local authorities to share data either internally or externally in reliance on section 111 of the Local Government Act 1972 or section 2 of the Local Government Act 2000. The power that is contained in section 2 of the Local Government Act 2000 is of particular relevance as it is designed to ensure that service delivery is co-ordinated in ways which minimise duplication and maximise effectiveness. More information about these powers is contained in Section 4.

Specific relevant administrative law

Part 1 of the Local Government Act 2000 gives local authorities powers to take any steps which they consider are likely to promote the wellbeing of their area or the inhabitants of it.

Section 2 gives local authorities ‘a power to do anything which they consider is likely to achieve any one or more of the following objectives’:

- the promotion or improvement of the economic wellbeing of their area;
- the promotion or improvement of the social wellbeing of their area;
- the promotion or improvement of the environmental wellbeing of their area.

Section 2 (5) makes it clear that a local authority may do anything for the benefit of a person or an area outside their area, if the local authority considers that it is likely to achieve one of the objectives of Section 2(1).

Section 3 is clear that local authorities are unable to do anything (including sharing information) for the purposes of the wellbeing of people - including children and young people - where they are restricted or prevented from doing so on the face of any relevant legislation, for example, the Human Rights Act and the Data Protection Act or by the common law duty of confidentiality.

Human Rights Act 1998 and the European Convention on Human Rights

The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable action within their powers (which would include information sharing) to safeguard the Convention rights of children. These rights include the right to life (Article 2), the right not to be subjected to torture or inhuman or degrading treatment (Article 3) and the right to liberty and security (Article 5).

Article 8 of the European Convention on Human Rights was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect for private and family life:

- Article 8.1: Everyone has the right to respect for his private and family life, his home and his correspondence.
- Article 8.2: There shall be no interference by a public authority with 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 crime or disorder, protection of health and morals, or for the protection of rights and freedoms of others.

Sharing confidential information may be a breach of an individual's Article 8 right: the question is whether sharing information would be justified under Article 8.2 and proportionate. You need to consider the pressing social need and whether sharing the information is a proportionate response to this need and whether these considerations can override the individual's right to privacy. If a child or young person is at risk of significant harm, or sharing is necessary to prevent crime or disorder, breach of the child or young person's right would probably be justified under Article 8.

Common Law Duty of Confidence

The common law protects from disclosure information (whether personal or not) that "is given in circumstances giving rise to an obligation of confidence on the part of the person to whom the information has been given". This means that where information is passed in circumstances where a confidential relationship has been established, the person receiving the information is under a duty not to pass on the information to a third party. But the duty is not absolute and information can be shared without breaching the common law duty if:

- the information is not confidential in nature; or
- the person to whom the duty is owed has given explicit consent; or
- there is an overriding public interest in disclosure; or
- sharing is required by a court order or other legal obligation

When considering disclosure, a judgment must be made as to where the public interest lies (the more sensitive and damaging the information, the stronger the public interest in disclosure will need to be).

Data Protection Act 1998

The Data Protection Act 1998 deals with the processing of personal data and provides individuals with a number of important rights to ensure that their information is processed lawfully. In general terms the Act regulates the manner in which personal data can be collected, used and stored and so is of prime importance in the context of information

sharing. Organisations who process personal data must comply with the 8 Data Protection principles laid down in the Act, these are:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed for any other purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of data subjects and therefore accessible to them
- Appropriate technical and organisational measures shall be taken to protect personal data from unauthorised or unlawful processing and from accidental loss, destruction or damage
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless they can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Crime and Disorder Act 1998

Section 17 applies to a local authority (as defined by the Local Government Act 1972); a joint authority; a police authority; a national park authority; and the Broads Authority. As amended by the Greater London Authority Act 1999 it applies to the London Fire and Emergency Planning Authority from July 2000 and to all fire and rescue authorities with effect from April 2003, by virtue of an amendment in the Police Reform Act 2002.

It recognises that these key authorities have responsibility for the provision of a wide and varied range of services to and within the community. In carrying out these functions, section 17 places a duty on them to do all they can to reasonably prevent crime and disorder in their area.

The purpose of this section is simple: the level of crime and its impact is influenced by the decisions and activities taken in the day to day business of local bodies and organisations. Section 17 is aimed at giving the vital work of crime and disorder reduction a focus across a wide range of local services that influence and impact upon community safety and putting it at the heart of local decision making. Section 17 is a key consideration for these agencies in their work in crime and disorder reduction partnerships, drug action teams, YOTs, children's trusts and local safeguarding children boards.

Section 37 sets out that the principal aim of the youth justice system is to prevent offending by children and young people and requires everyone carrying out youth justice functions to have regard to that aim.

Section 39(5) sets out the statutory membership of YOTs reflecting their responsibilities both as a criminal justice agency and a children's service

Section 115 provides any person with a power but not an obligation to disclose information to responsible public bodies (e.g. police, local and health authorities) and with

co-operating bodies (e.g. domestic violence support groups, victim support groups) participating in the formulation and implementation of the local crime and disorder strategy.

The police have an important and general common law power to share information to prevent, detect and reduce crime. However, some other public organisations that collect information may not have had the power previously to share it with the police and others.

Section 115 clearly sets out the power of any organisation to share information with the police authorities, local authority (including parish and community councils), Probation Service and health authority (or anyone acting on their behalf) for the purposes of the Act.

This ensures that information may be shared for a range of purposes covered by the Act, for example for the functions of the crime and disorder reduction partnerships and YOTs, the compilation of reports on parenting orders, anti-social behaviour orders, sex offender orders and drug testing orders.

National Health Service Act 1977

The Act provides for a comprehensive health service to England and Wales to improve the physical and mental health of the population and to prevent, diagnose and treat illness.

Section 2 provides for sharing information with other NHS professionals and practitioners from other agencies carrying out health service functions that would otherwise be carried out by the NHS.

Health Act 1999

Section 27 of the Health Act replaces section 22 of the NHS Act 1977. Section 27 states that NHS bodies and local authorities shall co-operate with one another (this allows for practitioners to share information) in order to secure the health and welfare of people.

Adoption and Children Act 2002

For further information about the Adoption and Children Act 2002 and Regulations see www.dfes.gov.uk/adoption/lawandguidance.

Police and Justice Act 2006

The implications of this include **Sections 7 to 9** which standardise the powers of Community Support Officers (CSOs) and provide a new power in relation to dealing with truancy, **Sections 23 to 25** which amend the provisions on parenting contracts and parenting orders in the Anti-Social Behaviour Act 2003 to provide that local authorities and registered social landlords can enter into parenting contracts and apply for parenting orders, and **Sections 39 and 40** which amend the Protection of Children Act 1978 to enable the forfeiture of indecent photographs of children irrespective of the power they have been seized under.

Individual's Rights & Responsibilities

In respect of the rights and responsibilities of children, young people and their families with regard to information sharing, the guidance issued by the Information Commissioner states that:

- a) A person of 12 years or more shall be presumed to be of sufficient age and maturity, and thus have a general understanding, to be able to exercise any right under the Act.
- b) For a person under 12 years of age someone with parental responsibility, or a guardian, may exercise those rights on behalf of the child.
- c) If a person aged 12 years or more is determined not to be capable of exercising their rights then a legal guardian may exercise those rights on their behalf.

This section provides guidance on the statutory powers that are of particular relevance to the delivery of the Wolverhampton MASH and the extent to which sharing of information is permitted by these statutory provisions.

Legislation	Duties
Localism Act 2011	For CoWC - Section 1 of the Localism Act 2011 as it provides a general power of competence "to do anything that individuals generally may do" (S1(1)) and "...to do it in any way whatever, including....(c) power to do it for, or otherwise than for, the benefit of the authority, its area or persons resident or present in its area."
Local Government Act 2000	For CoWC - If there are no relevant statutory restrictions it may then be possible for local authorities to share data either internally or externally in reliance on section 111 of the Local Government Act 1972 or section 2 of the Local Government Act 2000. The power that is contained in section 2 of the Local Government Act 2000 is of particular relevance as it is designed to ensure that service delivery is co-ordinated in ways which minimise duplication and maximise effectiveness.
Children Act 1989	<p>Section 17 – provides implied power for children's services to share information with other professionals who can assist in assessing whether a child is in need and to share information with agencies which provide services for children in need.</p> <p>Consent to share information should be obtained and recorded wherever possible. If a parent indicates that they do not wish to share information with a particular professional, their views should be considered but they are not determinative.</p> <p>If consent is not obtained information can still be obtained from other professionals, provided:</p> <ol style="list-style-type: none"> (a) A legal power to share information exists (Section 17 & Section 47 of the Children Act 1989 provides this power, as does Section 10 and Section 11 of the Children Act 2004) (b) Information is shared in compliance with the Data Protection Act

	<p>1998 (see below section DPA 1998)</p> <p>(c) Information that holds a duty of confidence is only shared if there is an overriding public interest or where permitted by a court order.</p> <p>(d) Information is necessary and proportionate and therefore does not contravene Article 8 of the Human Rights Act (HRA) 1989. Where information is being shared without consent, the parent/child needs to be informed of what action is being undertaken unless it is inappropriate to do so (unless this would put them at further risk, breach a duty of confidence or prejudice criminal investigations)</p> <p>(e) There is no statutory or court prohibition on information sharing.</p>
<p>Children Act 1989</p>	<p>Section 47 - Section 47 thresholds do not determine whether or not consent should be sought within MASH: It is inherent in the idea of seeking consent that it will be refused.</p> <p>If professionals consider it justifiable to override the refusal in the interests of the welfare of the young person or vulnerable adult then they can and must do so. This decision must be proportionate to the harm that may be caused by proceeding without consent.</p> <p>Where it is believed the aims of the MASH might be prejudiced if agencies were to seek consent the disclosing agency must consider the grounds to override the consent issue.</p> <p>The disclosure of personal information without consent is legally justifiable if it falls within one of the defined categories of public interest. The Public Interest Criteria includes:</p> <ul style="list-style-type: none"> • The administration of justice; • Maintaining public safety; • The apprehension of offenders; • The prevention of crime and disorder; • The detection of crime; • The protection of vulnerable members of the community. <p>When judging the public interest, the following will be considered:</p> <ul style="list-style-type: none"> • Is the intended disclosure proportionate to the intended aim? • What is the vulnerability of those who are at risk? • What is the impact of disclosure likely to be on the individual? • Is there another equally effective means of achieving the same aim? • Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public; • Is it necessary to disclose the information, to protect other vulnerable people?

	<p>A proportionality test must be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.</p> <p>Information is shared initially within the MASH with or without consent in order to assess risk and harm, which in turn identifies the proportionate level of response required.</p> <p>Once a decision is made based on this shared information picture, the relevant partner may hold back within the MASH any information which is deemed by the originating organisation to be too confidential for wider dissemination. Should it be decided to retain confidential information within the MASH then it must always be 'demilitarised' to any professional who may receive a referral or request for service.</p> <p>When overriding the duty of confidentiality, the MASH must seek the views of the organisation that holds the duty of confidentiality and take into account their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.</p> <p>All disclosures must be relevant and proportionate to the intended aim of the disclosure.</p>
<p>Children Act 2004</p>	<p>Section 10 –promote cooperation to improve wellbeing of children, including sharing of resources and information</p>
<p>Data Protection Act 1998</p>	<p>Under Schedule 2 of the DPA, either of the following conditions can be met:</p> <ol style="list-style-type: none"> 1. The data subject has given his implied consent to the processing through either agency's privacy notice (usually provided at the start of any service provision with the family/adult/child/young person) 2. The processing is necessary for the exercise of any functions conferred by or under any enactment (see above legislation) 3. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed. <p>Under Schedule 3, the following conditions can be met:</p> <ol style="list-style-type: none"> 1. The data subject has given explicit consent. 2. The processing is necessary for the exercise of any functions conferred by or under any enactment (see above legislation); <p>It is also important to ensure that other Data Protection principles are complied with, for example the information being shared is relevant to the purposes of this agreement and is not excessive; information being shared is accurate and up to date; information is kept for no longer than necessary; information shared is kept secure.</p>

Mental Capacity Act 2005	Section 4 Best interests
Care Act 2014	Sections 1-7, covering the promoting of best interests, giving of information and advice. Also Section 42-Enquiry by local authority.
Equality Act 2010	Chapter 2 provisions-prohibited conduct
Housing Act 2004	Enforcement provisions
Health & Social Care Act 2008, 2012, 2014	
The Health Act 1999	Section 31 – Arrangement between NHS Bodies and local authorities
NHS Act 1977	The Act provides for a comprehensive health service to England and Wales to improve the physical and mental health of the population and to prevent, diagnose and treat illness. Section 2 provides for sharing information with other NHS professionals and practitioners from other agencies carrying out health service functions that would otherwise be carried out by the NHS.

Appendix B: Information Sharing

Information sharing flowchart

It is acknowledged that sharing information requires exercising some judgement and, to assist with this, the recent HM Government guidance (published March 2015) has identified **seven golden rules** for practitioners to remember on information sharing in respect of children and young people and by definition, vulnerable adults as well. The principles are:

- Data Protection and Human Rights is not a barrier to sharing, they provide a framework to ensure sharing is necessary and proportionate.
- Be open and honest. You should explain to children, young people and their families at the outset, what and how information will, or could be shared and why, and seek their agreement. The exception to this is where to do so would put that child, young person or others at increased risk of significant harm, or an adult at risk of serious harm, or if it would undermine the prevention, detection or prosecution of a serious crime, including where seeking consent might lead to interference with any potential investigation.
- Seek advice from practitioners if you are in doubt about sharing information, while keeping matters anonymous if possible. You must always consider the safety and welfare of a child or young person when making decisions on whether to share information about them. Where there is concern that an individual may be suffering or is at risk of suffering significant harm, their safety and welfare must be the overriding consideration.
- Share with informed consent where possible. You should, where possible, respect the wishes of children, young people or their families who do not consent to share confidential information. You may still share information if, in your judgement on the facts of the case, there is sufficient need to override that lack of consent.
- Consider well-being and safety of individuals where sharing. Base your decisions upon this and document them
- You should ensure that the information you share is accurate and up-to-date, necessary for the purpose for which you are sharing it, shared only with those people who need to see it, and shared securely.
- You should always record the reasons for your decision - whether it is to share information or not.

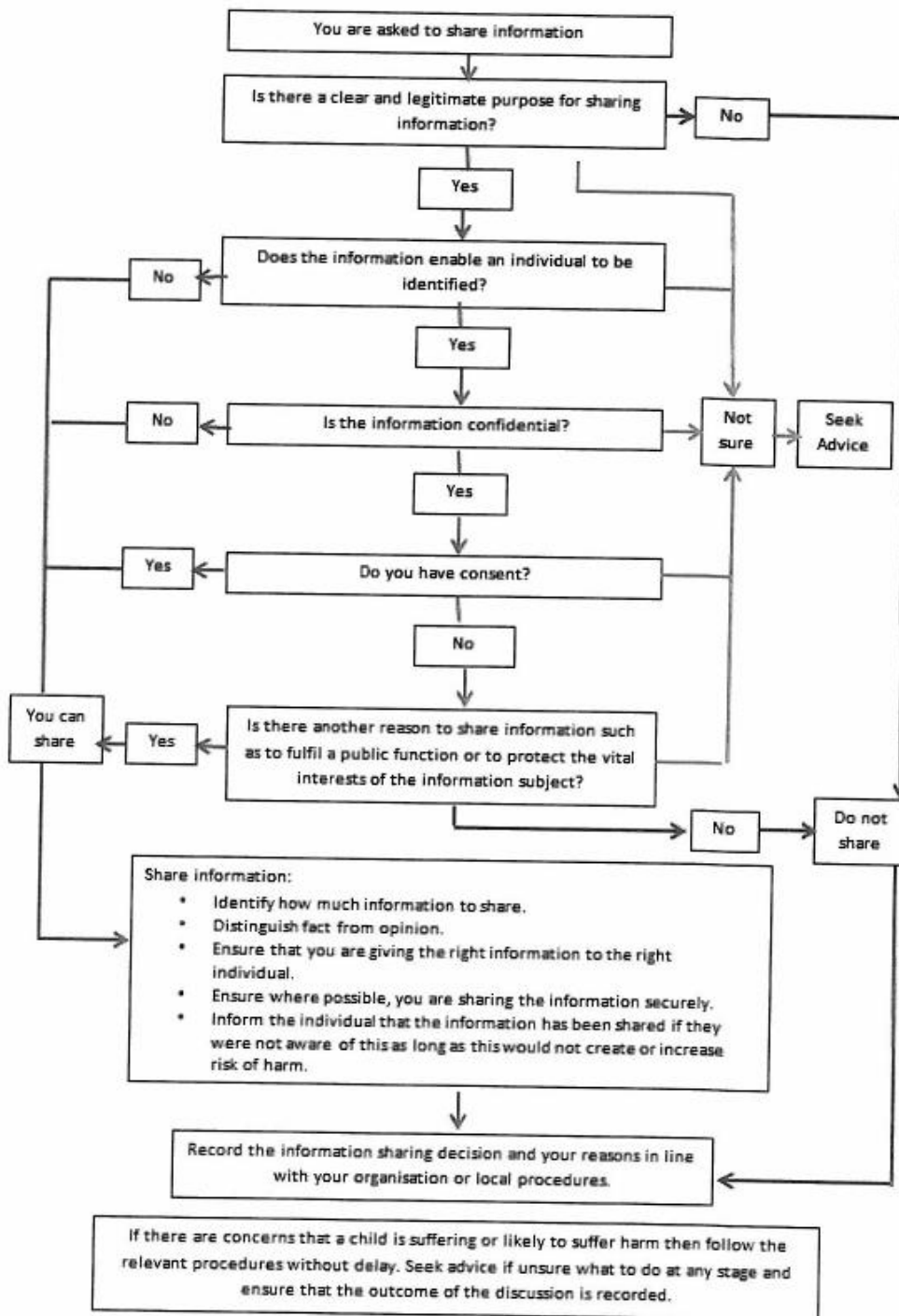
These principles are applied through **eight questions** set out below. The relationship between these questions is illustrated in the information sharing **flowchart overleaf**.

1. Is there a legitimate purpose for you or your agency to share the information?

2. Does the information enable a person to be identified?
3. Is the information confidential?
4. If the information is confidential, do you have consent to share it?
5. Is there a statutory duty or court order to share the information?
6. If consent is refused, or there are good reasons not to seek consent to share confidential information, is there a sufficient public interest to share it?
7. If the decision is to share, are you sharing the right information in the right way?
8. Have you properly recorded your decision?

(Note: The flowchart below relates to the HM Government guidance - **Information Sharing: Advice for practitioners providing safeguarding services to children, young people parents and carers** - published in March 2015)

Flowchart of when and how to share information



Appendix C – Multi Agency Referral Form (MARF) and SA1 form

The attachment and link below provides access to the current MARF (Childrens)

1. Identification of Children in Need of Protection and the Procedures for the Management of Individual Cases Where There Are Concerns About a Child's Safety and Welfare

The following link provides access to the latest SA1 (Adults) referral form:

<https://www.wolverhamptonsafeguarding.org.uk/index.php/safeguarding-adults/i-work-with-adults-with-care-and-support-needs/policies-and-procedures>

IMPORTANT: Once either version of the forms are completed, the appropriate Protective Marking classification of [PROTECT] or [RESTRICTED] should be applied.

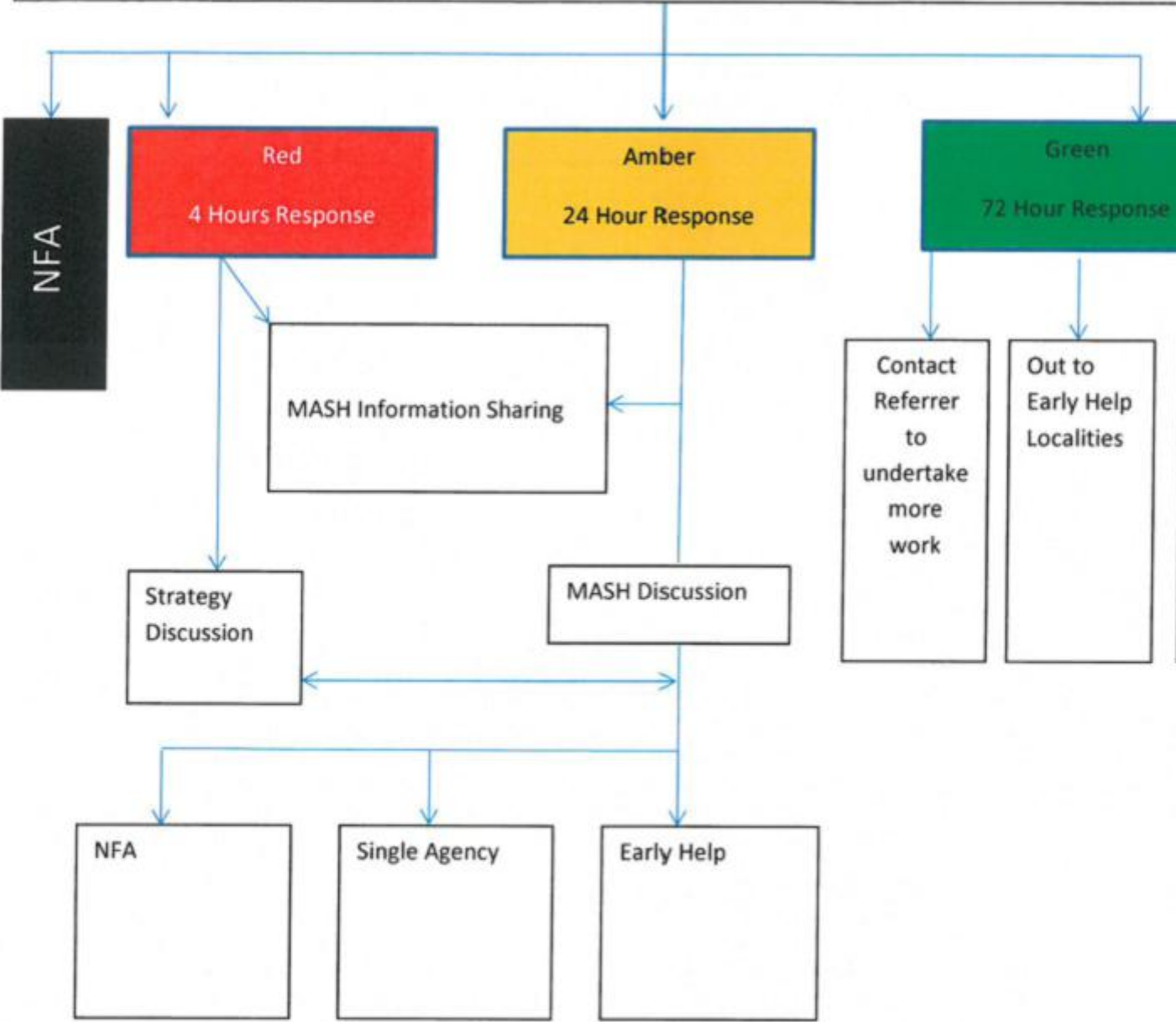
Appendix D: Information Governance Leads

Partner Agency	Name	Role	Contact Details
City of Wolverhampton Council	Anna Zollino-Biscotti	Information Governance Manager	01902-555166 Anna.zollino-biscotti@wolverhampton.gov.uk
The Royal Wolverhampton NHS Trust	Raz Bassi	Information Governance Manager	01902 307999 Raz.bassi@nhs.net
Wolverhampton CCG	Peter McKenzie	Information Governance Lead/POC	peter.mckenzie2@nhs.net
Black Country Partnership Foundations Trust	Katie Sparrow	Information Governance Manager	Katie.sparrow@bcpft.nhs.uk
Wolverhampton Homes	Angela Barnes	Information Governance POC	Angela.Barnes@Wolverhamptonhomes.org Angela.barnes@wolverhampton.gov.uk
YOW (& Voluntary Sector)	Stephen Dodd	Information Governance POC	Tel: 01902 877545 steve@yow.org.uk
Police	Corrina Griffiths	Information Governance POC	Corrina.griffiths@west-midlands.pnn.police.uk
Probation	Jamie Ann Edwards Jacqui Thompson	Information Governance POC	Jamie-Ann.Edwards@swm.probation.gsi.gov.uk jacqui.thompson@swm.probation.gsi.gov.uk
West Midlands Fire	Kate Houghton	Information Governance POC.	Kate.houghton@wmfs.net
Recovery Near You	Helen Kilgallon	Information Governance POC.	helen.kilgallon@nacro.org.uk

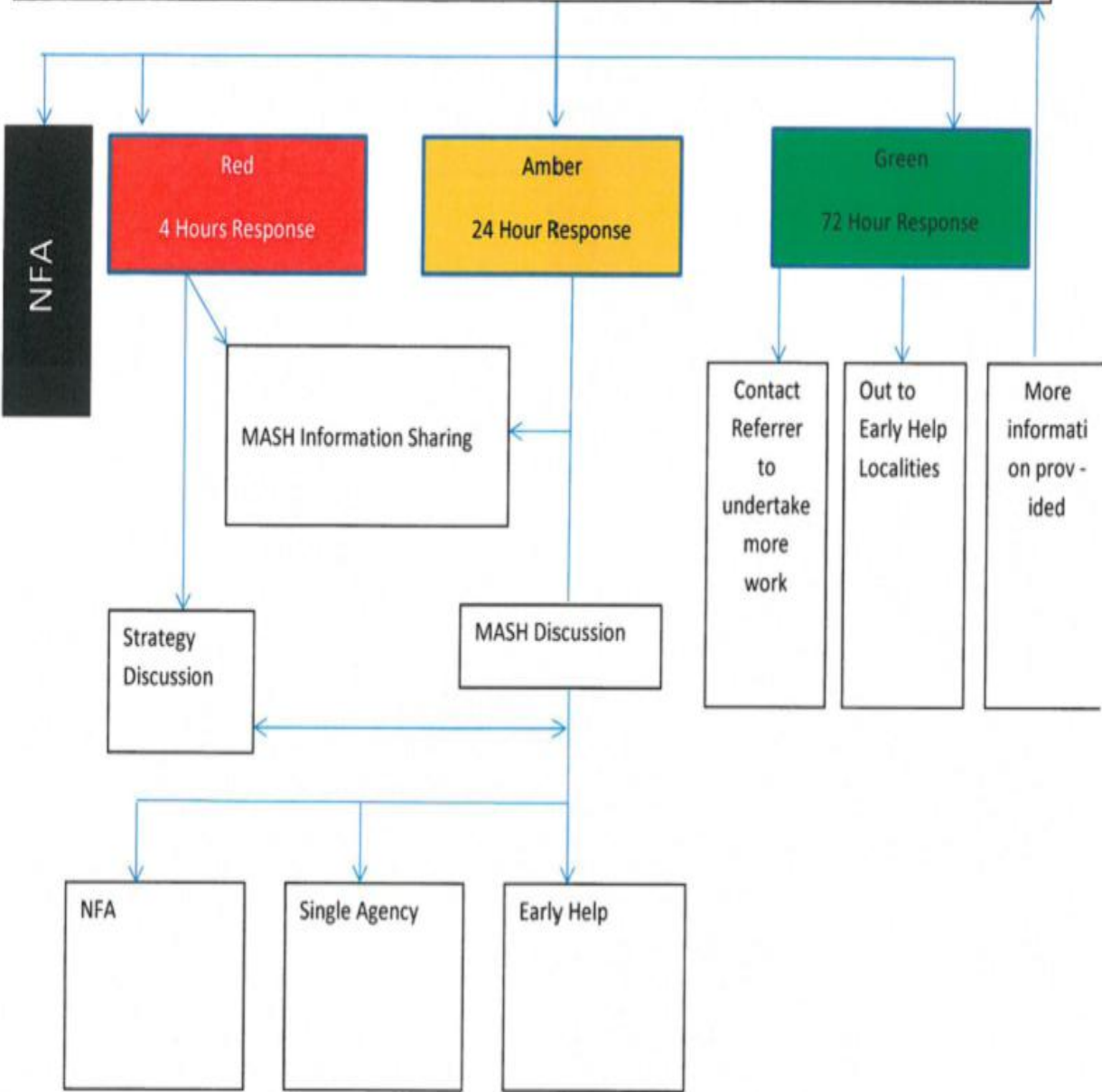
POC = Point of Contact

Appendix E: Children’s MASH Process Map

Concern about a Child or Young Person is reported.
MASH Screening Officers undertake Initial Information Sharing.
EH/SC Lead Professionals review information/referral and apply RAG rating and threshold.



Concern about a Child or Young Person is reported.
MASH Screening Officers undertake Initial Information Sharing.
EH/SC Lead Professionals review information/referral and apply RAG rating and threshold.



Appendix F Adults MASH Process Map

Wolverhampton Multi-Agency Safeguarding Hub (MASH) - Adults

