BIRMINGHAM SAFEGUARDING CHILDREN BOARD

INFORMATION SHARING PROTOCOL

CONTENTS

1. Purpose of this Protocol
   - Limits of this Protocol
2. The Legal Basis for Information Sharing under this Protocol
3. Privacy Notices
4. Responsibilities of Individual Staff
5. Sharing Personal Information with Consent
6. Sharing Information when there are Significant Concerns about a Child's Welfare
7. Further Information Sharing under this Protocol
   In the absence of specific concerns or explicit consent.
8. The Process of Sharing Information
   - Personal information that may be shared
   - The legal basis for sharing information
   - The process of sharing information
   - How the information may be shared
   - Retention and further use of information
   - Recording the decision
9. Partner Agencies' Responsibility for Security of Information
   - Information security breach
10. Review Arrangements
11. Agreement to Abide by this Protocol
12. Signatories

APPENDICES

Appendix A: Glossary of Terms and Abbreviations
Appendix B: Guidance Related to Information Sharing

1. PURPOSE OF THIS PROTOCOL

This Protocol has been developed to set out –

- The purposes for which the signatory agencies have agreed to share personal information;
- The circumstances in which the signatory agencies may need to share personal information;
- The personal information that may be shared between the signatory agencies;
- The process for sharing personal information;
- The responsibility of signatory agencies to ensure the security of personal information; and
- The action to be taken if the requirements of this Protocol are not met.

The signatories to this Protocol will represent the following partner agencies of Birmingham Safeguarding Children Board:

- Birmingham City Council.
- West Midlands Police.
- NHS Organisations in Birmingham
- The National Probation Service
- The Child and Family Court Advisory and Support Service
- Staffordshire and West Midlands Community Rehabilitation Company
- West Midlands Fire Service
- Schools (maintained schools, academies, free schools and independent schools).

All future additional partner agencies joining Birmingham Safeguarding Children Board will be required to sign up to this Protocol as part of the conditions for their joining.

Limits of this Protocol

This Protocol does not apply to actions taken within the Multi-Agency Safeguarding Hub (MASH). The MASH has its own Information Sharing Protocol covering its internal business.

2. THE LEGAL BASIS FOR INFORMATION SHARING UNDER THIS PROTOCOL

All organisations are subject to a variety of legal, statutory and other guidance in relation to the sharing of person-identifiable or anonymised data. For the Signatory Parties to this Protocol the key legislation affecting the sharing and disclosure of data includes (but this is not necessarily an exhaustive list): -

- The Mental Health Act 1983
- The Access to Health Records Act 1990
- The Data Protection Act 1998
- The Crime and Disorder Act 1998

- The Human Rights Act 1998
- The Local Government Act 2000
- The Education Act 2002
- The Freedom of Information Act 2000
- The Homelessness Act 2002
- The Criminal Justice Act 2003
- The Children Act 2004
- The Civil Contingencies Act 2004
- The Mental Capacity Act 2005
- The Safeguarding Vulnerable Groups Act 2006
- The Health and Social Care Act 2012
- The Common Law Duty of Confidentiality

The Signatory Parties to this Protocol consider that the statutory provisions listed above are likely to permit the sharing of personal information, depending upon the specific circumstances of each particular case.

3. PRIVACY NOTICES

It is a requirement of the Data Protection Act 1998 that all organisations that process Personal Data should have what is now known as a Privacy Notice. This will inform individuals about how their Personal Data will be used by that organisation. The notice will cover:

- The identity of the data controller;
- The purpose or purposes for which you intend to process the information;
- Details of the parties with whom information may be shared; and
- Any further information you need to give data subjects so that the data will be processed fairly.

Each Partner Agency will ensure that their Privacy Notice is consistent with this Protocol.

4. RESPONSIBILITIES OF INDIVIDUAL STAFF

Every individual working within the Partner Agencies is personally responsible for the safekeeping of any information they obtain, handle, use and disclose. Every individual should:

- Know how to obtain, use and share the information they legitimately need to do their job;
- Uphold the general principles of confidentiality, seeking advice when necessary; and
- Be aware that any violation of privacy or breach of confidentiality is potentially a disciplinary matter and may be unlawful. Criminal proceedings might be brought against the individual responsible for the breach.

5. SHARING PERSONAL INFORMATION WITH CONSENT

The Data Protection Act 1998 allows that Personal Data may be shared with the consent of the data subject. If the Personal Data is sensitive, then explicit consent must be given. In the case of Personal Data relating to a child, if the child has capacity to give or withhold consent, s/he may do so. If the child lacks capacity to decide on the matter, or does not wish to make a decision, then a person who holds parental consent for the child may give or withhold consent on the child's behalf.

The meaning of "consent" in this context is discussed on the website of the Information Commissioner's Office.

If the data subject gives explicit consent to the sharing of personal information between agencies, then it may be shared between Partner Agencies, subject to any limits set by the data subject. The person providing information to, or requesting information from, another agency should state clearly that consent has been given, and by whom.

The process for sharing information between Partner Agencies is set out in Section 8 of this Protocol.

6. SHARING INFORMATION WHEN THERE ARE SIGNIFICANT CONCERNS ABOUT A CHILD'S WELFARE

When there is evidence that a child may be at risk of significant harm, and the sharing of personal information between Partner Agencies is necessary in order to quantify that risk, or to decide on the appropriate action to take, then Personal Data should be shared, with or without consent. If consent has not been given, information should only be shared with those who need to know it in order to assess the level and type of any risk to the child's welfare and to respond to it; and the information that should be shared is limited to what is relevant to the issue of risk to the child. Need to know is defined in terms of adequately protecting the child from harm.

When information sharing is necessary in order to assess whether a child is at risk of significant harm, or to decide on the appropriate action to take in response to such risk, then it must be shared between Partner Agencies, subject to the "need to know" limitations described above. The person offering information to, or requesting information from, another agency should state clearly whether consent to the sharing has been given and, if not, the circumstances that justify sharing without consent.

The process for sharing information between Partner Agencies is set out in Section 8 of this Protocol.

When the national "Child Protection – Information Sharing" project extends to Birmingham it will be subject to this Protocol. Information sharing in this scheme will be justified because of existing concerns about the child's welfare.

7. FURTHER INFORMATION SHARING UNDER THIS PROTOCOL
In the absence of specific concerns or explicit consent

Personal information, including sensitive Personal Data, may be shared between Partner Agencies without consent if the sharing is necessary for the exercise of any functions conferred on any person by an enactment. In addition the Board itself can require an individual or body to comply with a request for information if the information is needed for the purpose of enabling or assisting the Board to perform its functions (Children Act 2004, Section 14B). For example the Local Safeguarding Board Regulations 2006 state that the functions of a Local Safeguarding Children Board will include undertaking reviews of serious cases and collecting and analysing information about each death of a child normally resident in the Board's area. Information sharing is therefore justified where it is necessary for:

- The work of the Child Death Overview Panel;
- The Sudden Unexpected Death in Infancy process; and
- A Serious Case Review.

The sharing of personal information is not justified if the legal responsibilities could adequately be met by the provision of anonymised information.

8. THE PROCESS OF SHARING INFORMATION

All decisions to share or not to share information under this Protocol must be decided on a case-by-case basis and a written record must be retained giving details of the reasons for sharing, what information was shared, with whom and when.

Personal information that may be shared

The information that may be shared under this Protocol will comprise the following fields in relation to children, their siblings, family members and others who have contact with them, or are likely to have future contact with them:

- Name;
- Date of birth;
- Place of residence;
- Next of kin;
- Details of family members;
- Physical and/or mental health conditions;
- Religious beliefs;
- Ethnicity;
- Education/school;
- Details related to alleged, suspected or actual harm, abuse, neglect etc.;
- Details of alleged, suspected or actual perpetrators of harm, abuse or neglect.

The information may be shared by a Partner with one or all of the Partner Agencies, or with the Board's business support team, as appropriate.

The legal basis for sharing information

Before sharing personal information, both the Disclosing Party and the Receiving Party must ensure that they understand whether the sharing is justified by –

- The consent of the data subject; or
- Concern about the welfare of a child;
- The legal responsibilities of the relevant Partner Agency; or
- The legal responsibilities of the Safeguarding Children Board.

The process of sharing information

When a person or agency wishes to share information with another agency under this Protocol they should state clearly why this is necessary in order to carry out the Board's legal responsibilities and/or the responsibilities of the Disclosing Party and the Receiving Party.

The Disclosing Party will select the information to be disclosed on the basis that disclosure is necessary and proportionate and that the specific information is:

- Relevant;
- Adequate;
- Accurate; and
- Timely.

Both the Disclosing Party and the Receiving Party will ensure that all information is shared securely, each following their own agency's policy on security for handling personal information.

How the Information may be shared

Information shared under this Protocol may be shared by the following methods:

- During discussions in person or by telephone between the appropriate persons, with a written record of the shared information being made and retained;
- Secure encrypted email with the encryption key/password provided separately to the recipient by telephone;
- By NHSMail using the [Secure] encryption function in the subject field;
- By NHSMail to NHSMail – no password is necessary for this;
- By any other suitably secure method agreed in advance, preferably in writing, by the Disclosing Party and the Receiving Party.

Retention and further use of information

When information is shared under this Protocol, the Disclosing Party and the Receiving Party will agree –

- How the Receiving Party will use the information, including any further disclosure on to other agencies; and
- The period for which the Receiving Party intends to retain the information.

In some situations the Disclosing Party may require that the information provided will not be placed on the Receiving Party's records and that all copies will be either destroyed or returned by a set date.

Recording the decision

Both the Disclosing Party and the Receiving Party will record the decision to share, or not to share information, and the reasons for it.

9. PARTNER AGENCIES' RESPONSIBILITY FOR SECURITY OF INFORMATION

Partner Agencies to this Protocol will communicate the Protocol to their staff, and will provide appropriate training to them in respect of Data Protection, Human Rights and the Common Law Duty of Confidentiality. Records of such training must be maintained.

On receipt of Personal Data shared under this Protocol, the Receiving Party becomes a Data Controller and is therefore legally responsible for compliance with the Data Protection Act 1998 in respect of that Personal Data. Each Partner Agency signed up to this Protocol is responsible for ensuring that technical and organisational measures are in place to protect the security and integrity of the Personal Data that they hold and that their staff are properly trained to understand their responsibilities and comply with the law.

Partner Agencies will accept the security levels on information supplied by other partners and will handle the information accordingly. Partner Agencies accept responsibility for independently or jointly auditing compliance with this Protocol within reasonable time-scales. In particular all parties to this Protocol must have in place, implement, maintain and comply with the following minimum standards in respect of Personal Data -

- All mobile and portable electronic devices processing Personal Data shall be encrypted and such devices shall be securely stored when not in use.
- All electronic devices processing Personal Data shall require password authentication and all users shall be required to have unique usernames.
- All paper copies of Personal Data shall be securely stored when not in use.
- Personal Data, whether stored on paper or electronically, shall not be left unattended in vehicles.
- Access to Personal Data shall be on a need to know basis.
- Agencies will maintain policies that set out requirements in respect of remote or home working, sending Personal Data by email or fax, the retention, weeding and secure waste destruction of Personal Data;

Partner Agencies should make it a condition of employment that employees will abide by their agreed rules and policies in relation to the protection and use of Personal Data and Confidential Information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's procedures. Furthermore, Partner Agencies should ensure that their contracts with external service providers require

compliance with their rules and policies in relation to the protection and use of Confidential Information.

Information Security Breach

For the purposes of this Protocol an actual or suspected information security breach has occurred when any employee/contractor of a Partner Agency has reason to believe that an information system has been accessed by unauthorised individuals or when an employee/contractor of a Partner Agency has reason to believe that Confidential Information and/or Personal Data has been disclosed to a person not authorised to receive it. Examples of information security breaches which require immediate reporting include:

- Loss or theft of media containing Confidential Information or Personal Data. This could include paperwork, files, electronic equipment such as laptops, PDAs, or any storage device.
- Suspected access or use of Confidential Information or Personal Data inconsistent with agency responsibilities, such as an employee who uses an assigned account to access records for personal or unapproved reasons.
- Access to information systems to which a user is not authorised. This can be through password sharing or guessing as well as a number of other methods.
- Sending Confidential Information or Personal Data to unauthorised recipients. This can be by letter, email, web access or direct information sharing, or any other method used for communication.

Actual or suspected breaches of security or confidentiality or other violations of this Protocol must be reported in line with each Partner Agency's incident reporting procedures. The Agency becoming aware of a breach must inform any relevant Partner Agencies within two working days of the initial report.

Investigations into breaches should be undertaken promptly and updates regarding the progress of such investigations should be provided to the Partner Agencies on a monthly basis.

10. REVIEW ARRANGEMENTS

Each Partner Agency should report on the effectiveness of their policy and procedure for sharing information as part of their annual s11 or s175 audit to Birmingham Safeguarding Children Board. The Board will use this information to sample the practice in each agency. The Board's business unit will produce an annual report to provide feedback to partners on the overall effectiveness of agencies' policies and any weaknesses that exist in policy or practice.

This Protocol will be formally reviewed annually by the Board, unless new or revised legislation or national guidance necessitates an earlier review. Any of the signatories may request an extraordinary review at any time when joint discussion and/or a joint decision is necessary to address local service developments. Reviews will be coordinated by the Practice Standards and Procedures Sub-Group.

11. AGREEMENT TO ABIDE BY THIS PROTOCOL

The agencies signing this Protocol accept that it provides a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities. They undertake to:

- Implement and adhere to the requirements set out in this Protocol;
- Ensure that where these requirements are complied with, then no restriction will be placed on the sharing of information other than those specified within this Protocol; and
- Engage in an annual review of this Protocol with partners.

12. SIGNATORIES

This Protocol shall be signed and issued by the key representatives of the relevant Partner Agencies as outlined in Part 1 of this Protocol.

By signing you confirm that you have read and understood the contents of this Protocol and that your organisation has implemented and will maintain controls and countermeasures outlined in this Protocol.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this Information Sharing Protocol.

APPENDICES

April 2015

APPENDIX A - GLOSSARY OF TERMS AND ABBREVIATIONS
Used in this Protocol

Interpretation In this Protocol use of the singular includes the plural and vice versa.

Accessible Record – means unstructured personal information usually in manual form relating to health, education, social work and housing.

The Board – means Birmingham Safeguarding Children Board.

Child - means any person aged under eighteen, that is from birth until their 18th birthday: however the arrangements made under this protocol may include arrangements relating to services for:

- Young people aged 18 – 19;
- Young people under 25 who are receiving services as care leavers; and
- Young people under 25 who are receiving services related to learning difficulties.

Confidential Information - means information in whatever form relating to a Partner Agency or to a person (whether living or deceased), which –

- Is not in the public domain;
- Has the necessary quality of confidence; and
- Was imparted in circumstances giving rise to a duty of confidence.

It includes, without limitation, information in written, oral, visual or electronic form or on any magnetic disc or memory wherever located.

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.

It includes any complete or partial copy of the information.

Consent – Issues of consent are discussed on the website of the Information Commissioner's Office.

Data – means information that is:

a) Being processed by means of equipment operating automatically; or
b) Recorded with the intention it be processed by such equipment; or
c) Recorded as part of a relevant filing system; or
d) Not in a or b or c, but forming part of an accessible record; or
e) Held by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller – is a person or a legal body such as a business or public authority who jointly or alone determines the purposes for which Personal Data is processed.

Data Processing – means any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Subject – is an individual who is the subject of personal data.

Disclosing Party – means the Partner Agency or other Third Party disclosing Confidential Information and/or Personal Data under this Protocol.

Disclosure – means the passing of information from the Data Controller to another organisation / individual.

DPA – means the Data Protection Act 1998.

European Economic Area (EEA) – this consists of the EU members together with Iceland, Liechtenstein and Norway.

Health Professional – in the Data Protection Act 1998 "health professional" means:

- Any person who is registered as a medical practitioner, dentist, optician, optometrist, pharmacist, pharmacy technician, nurse, midwife, osteopath or chiropractor; or
- Any person who is registered as an arts therapist, chiropodist; clinical scientist; dietitian; medical laboratory technician; occupational therapist; orthoptist; paramedic; physiotherapist; prosthetists; and orthotist; radiographer; or speech and language therapist; or
- A child psychotherapist.

Human Rights Act - means the Human Rights Act 1998.

MASH means the Multi-Agency Safeguarding Hub.

Partner Agency – means an organisation which is a partner agency of Birmingham Safeguarding Children Board.

Personal Data – is data which relate to a living individual who can be identified –

- 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.

Processing data – means performing any operation on data. The main examples are collect, retain, use, disclose and delete.

Receiving Party – means the Partner Agency who has received Confidential Information and/or Personal Data shared under this Protocol.

Relevant Filing System means a set of information relating to individuals which is not processed automatically, but is structured in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data – The DPA defines sensitive Personal Data as information about:

(a) The racial or ethnic origin of the data subject;
(b) His political opinions;
(c) His religious beliefs or other beliefs of a similar nature;
(d) Whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
(e) His physical or mental health or condition;
(f) His sexual life;
(g) The commission or alleged commission by him of any offence; or
(h) 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.

Third Party – means any person who is not the data subject, the data controller, or the data processor.

APPENDIX B - GUIDANCE RELATED TO INFORMATION SHARING

Working Together to Safeguard Children [2015] states that –

> In addition, the LSCB can require a person or body to comply with a request for information. This can only take place where the information is essential to carrying out LSCB statutory functions. Any request for information about individuals must be 'necessary' and 'proportionate' to the reasons for the request. LSCBs should be mindful of the burden of requests and should explain why the information is needed.
>
> Chapter 3 Paragraph 22

HM Government has published guidance which should be read in conjunction with this Protocol.

- Information Sharing: Advice for practitioners providing safeguarding services to children, young people and parents [March 2015].

Attention is particularly drawn to the "seven golden rules of information sharing" set out in the this guidance.

The Information Commissioner (who is responsible for regulating and enforcing the DPA) has produced a statutory Data Sharing Code of Practice which also offers useful guidance:

- Data Sharing Code of Practice [May 2011]

This includes a statement of the 8 Data Protection Principles.

The Website of the Information Commissioner's Office includes information about:

- The Data Protection Principles
- The common law duty of confidence
- Consent

These documents should be considered as useful guidance in respect of the legal principles and of what the law requires with regard to decisions about the sharing of information, but they do not constitute legal advice. If any Party to this Protocol is unsure about the legal basis for specific information sharing they should seek advice from their own information governance officers or lawyers.