INFORMATION SHARING WITHIN THE COMMUNITY

Information Sharing Protocol

Safeguarding Adults

Version: 3.6

Date: 7th October 2013

Owner: Birmingham Safeguarding Adults Board

Safeguarding: Document History

Date	Version	Summary of Changes	Changes marked
11 Jan 2007	1.0	Initial Draft	
14 Feb 2007	1.1	Revision to definitions	PW/PR/JS
29 Mar 2007	1.2	Revision in light of changes to national guidance	PW/PR/JS
8 Nov 2007	1.3	Update terminology and references	PW/MP
11 Dec 2007	1.4	Revision after Working Group meeting 21/11/07	PW/AGB
27 Feb 2008	2.0	Revision after Board meeting 25/01/08	PW/JS/MP
7 Mar 2008	2.1	Revisions per Debbie Talbot	DT/JS/MP
9 Mar 2008	2.2	New Para added to bottom of Section 10	AGB
12/3/08	2.3	Revisions to be accepted by Board members	
10 Sept 2012	3.0	Review of Protocol with BCC Legal department	
10 Sept 2012	3.1	Update of definitions	
09 Oct 2012	3.2	Partner agencies updated	
17 Oct 2012	3.3	Partner agencies updated	
31 Oct 2012	3.4	Partner agencies updated	
August 2013	3.5	Legal amends and updated terminology to be accepted by Board members	

07/10/2013 3.6 Amends to the reference section/final document to be ratified at BSAB meeting in November 2013

Approvals
This document requires approval by Birmingham Safeguarding Adults Board

Date of Approval **TBA**

Distribution

This document has been distributed to

Recipient	**Issue date**	**Version**
Chairs of Safeguarding Committees		
Representatives of Partner Agencies	April '07	1.2
Safeguarding Adults - subgroup	21/11/07	1.3
Birmingham Safeguarding Adults Board	25/01/08	1.4
Birmingham Safeguarding Adults Board	29/02/08	2.0

This is a Controlled Document.
On receipt of a new version, destroy all previous versions.
Information Sharing Protocol on Safeguarding Adults

Version: 3.6

Note on changes to approved document v2.0 of 28/03/2008

Section	**Change**
3	Additional definitions : Data Controller, Data Processor, Data Subject
4a	Add "regulation" to para 1
9	Revised wording to "Data Protection Act 1998" re: data processors
9	Revised wording to "Exemptions under Data Protection Act 1998" re: written record of why a disclosure was made
9	Revised wording to "Section 29" on disclosure to police
10	Update of partner organisations
12	Revised wording to "minimum expectation" re: portable media
13	Revised procedure on "Breach Management"

Version: 3.3

Section	Change
10	Birmingham and Solihull NHS Cluster added into the protocol

Version: 3.4

Section	Change
10	Birmingham East and North Primary Care Trust-removed Heart of Birmingham Primary Care Trust-removed South Birmingham Primary Care Trust-removed Birmingham and Solihull NHS Cluster added into the protocol

Version: 3.5

Section	Change
All document	Term 'vulnerable adult ' updated to 'adult at risk'
3	Definitions: Inserted text on adults at risk
4b	Additional wording under Professional Involvement (paragraph 4) and additional paragraph 6
5a	Revised wording under Seeking Consent for Information sharing
5c	Revised wording under Mental Capacity and Consent paragraph2
5d	Revised wording to Refused Consent , first paragraph
7	Revised wording to Framework for Information Sharing, final paragraph
9	Revised wording to Data protection Act 1998, additional paragraph on personal data
9	Revised wording under Schedule 2 of the Act on disclosure of sensitive , personal data paragraphs 1 and 2
9	Revised wording Section 29 Crime and taxation
9	Revised wording Section 31 Regulatory Activity
10	Updates to agency titles and additional statement re inclusion in contracts
11	Revised wording to Implementation, Monitoring and Review
13	Revised wording under Breach management

Version: 3.6

Section	Change
Sub appendix 4	Additional references added
10	Updated list of agencies

Index

1. Scope

Adult service users receive support and help from people in many agencies and organisations. The sum of the collective knowledge held by professionals provides a holistic view of their needs, family and support context and an understanding of what services they need to live in their chosen surroundings.

This document specifies the protocols to be used to enable improved information sharing among agencies and professionals who work with adults. It is intended to support the multi-agency procedures published to clarify the roles and responsibilities of professionals, staff or volunteers when faced with suspected abuse or inadequate care of a vulnerable adult/adult at risk (Safeguarding Adults 2005, No Secrets 2000). Information may also be shared if action needs to be taken on a preventative basis.

The protocol applies to all vulnerable adults/adults at risk living in Birmingham and those citizens living outside the area in care homes and care homes with nursing which are funded by Birmingham City Council. The authority where the abuse occurs will have overall responsibility for co-ordinating the Safeguarding Adult arrangements. The placing authority will have a continuing duty of care.

The protocol has been written with the understanding that the principles and standards defined in the overarching "General Protocol for Sharing Information between the Birmingham Health Community and Social Care and Health" (February 2004) will be applied throughout the processes it describes.

2. Objectives and Purpose

2a Protocol Objectives

To set out a framework to permit the secure, lawful and confidential sharing of information between organisations, to enable them to have adequate and accurate information to allow them meet the needs of vulnerable adults/adults at risk in accordance with national and local policy and legislative requirements (Safeguarding Adults 2005; No Secrets 2000 and the Mental Capacity Act 2005).

To inform members of the community why information about them may need to be shared and how this sharing will be managed.

2b Protocol Purpose

This Document:

2b.1 Outlines the procedures which will ensure that information is disclosed in line with organisational responsibilities.

2b.2 Identifies the reasons why information needs to be shared in order to provide protection for vulnerable adults/adult at risk in the community and who it will need to be shared with.

2b.3 Lists the organisations which have agreed to share information, where they consider that the sharing of information is fair and lawful, as described within this protocol.

2b.4 Describes the detail of the specific arrangements for each identified purpose for information sharing.

2b.5 Sets out factors that may support the organisations in reaching a decision as to whether or not to share Information, and does not seek to undermine the legal responsibility of each organisation, as a Data controller, to determine how and why personal data is processed or shared.

3. Definitions

In this document, the term **Safeguarding Adults** represents an ethos that is used to enable an adult "who is or may be eligible for community care services" to retain independence, wellbeing and choice and to access their human rights to live a life that is free from abuse and neglect. All persons have the right to live their lives free from violence and abuse. This right is underpinned by the duty on public agencies under the Human Rights Act 1998 to intervene proportionately to protect the rights of citizens.

'Vulnerable adults' is used to refer to any person aged 18 years and over who:

- Is or may be in need of community care services because of frailty, learning or physical disability, sensory impairment or mental health difficulty and
- Is or may be unable to take care of him/herself or take steps to protect him/herself from significant harm or exploitation.

[as quoted by Law Commission, 'Safeguarding Adults' and 'No Secrets' 8-9]

Please note: in the 'Safeguarding adults: multi-agency policy and procedures for the West Midlands' implemented in April 2013 the term 'adult at risk' is used as a replacement for the term 'vulnerable adult' and is therefore used throughout this document.

The concept of **significant harm** was introduced as the threshold that justifies compulsory intervention in the best interests of the adult at risk. The local authority is under a duty to make enquiries, or cause enquiries to be made, where it has reasonable cause to suspect that an adult at risk is suffering or likely to suffer, significant harm. To make enquiries involves assessing what is happening to the adult at risk. Where enquiries are being made, the assessment or investigation should concentrate on the harm that has occurred or is likely to occur to the adult at risk as a result of the alleged

incident(s) or neglect, in order to inform future plans and the nature of services required. Decisions about significant harm are complex and should be informed by a careful assessment of the adult at risk's circumstances, and discussion between the statutory and voluntary agencies and with the adult at risk, her/his advocate [where appointed] and family under the multi-agency Safeguarding procedure.

The term **investigation** or **assessment** is used in this protocol to cover any part of the safeguarding process from initial information gathering, enquiries about alleged incidents and relevant background, safeguarding meetings, investigations of possible abuse or harm, reviews and action planning.

Data controller means (under the Data Protection Act 1998) a person who - either alone or jointly or in common with other persons - determines the purposes for which and the manner in which any personal data are, or are to be, processed. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the Data controller.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data subject means an individual who is the subject of personal data.

4. Purposes and Professional Involvement

4a Purposes

In order to deliver services that protect the adult(s) at risk from abuse, risk or harm, the organisations party to this protocol may consider it appropriate, where it considers it fair and lawful, to share information about the adult(s) at risk, and other individuals having interaction with the adult(s) at risk between the agencies that provide and support and / or regulate these services.

Under the terms of this protocol, information will only be shared for the following purposes:

4a.1 In order to facilitate specific assessment / investigation where an allegation has been made or there is concern that abuse is taking place.

4a.2 In order to evaluate the outcome of such assessment / investigation and the effectiveness of the interventions provided

4a.3 In order to highlight or address risks to others that may have been identified in the course of an assessment / investigation.

4b Professional Involvement

Only those who need to know in order to perform a professional duty in relation to the adult at risk will join the information sharing network for sharing information about that case.

Only relevant information will be shared. Therefore there will be different levels of access operating in respect of each adult at risk, with minimal information held centrally.

The levels of information sharing will be based on the requirement to protect adults from risk of harm, and is determined by the disclosing organisation, i.e the Data controller who holds the information.

When sharing information with another agency it should be made clear, by the recipient, if there is any intention to pass it on to other agencies or persons. This may include all the agencies which take part in a multi-agency Safeguarding assessment / investigation, strategy discussion / meeting or case conference or review. Further information sharing should be within the limits of the given consent.

In practice this issue is most likely to present problems in relation to sharing information about alleged perpetrators. Within the boundaries of strict confidentiality of a multi-agency Safeguarding meeting there is justification for sharing information about an alleged perpetrator.

Any professional involved in sharing information about adult at risks must have undergone relevant training on sharing confidential information.

5. Consent for Information Sharing

5a Seeking Consent for Information Sharing

Initial information gathering after a report of an alleged incident may start before the consent of the adult at risk has been or can be sought.

Consent from the adult at risk (subject to the provisions of 5c below~) should be sought prior to sharing information within or between agencies, unless seeking that consent would be likely to cause or increase the risk of harm, either to the adult at risk or another person. The adult at risk will be given a full explanation as to why the information needs to be shared and who will have access to it.

5b Delays in Seeking Consent

In cases where there is a perceived risk of further harm to the adult at risk, the seeking of consent may be delayed or omitted at this point. In cases where

there is a perceived risk of compromising the assessment / investigation, the seeking of consent may be delayed or omitted at this point.

The reasons for any delay or omission should be evidenced and recorded.

5c Mental Capacity and Consent

If it is considered that the adult at risk may have difficulties in giving such consent, the organisation's procedures on Mental Capacity should be followed. However, it should be noted that the adult at risk is assumed to have capacity to give consent and that a lack of capacity should be clearly evidenced and recorded.

If it is decided that the adult at risk lacks capacity in accordance with the Mental Capacity Act to give informed consent to the sharing of their information, then any decision taken on their behalf must be in their best interests. Details of the Mental Capacity procedures can be found on www.birmingham.gov.uk/adults as a link on the Our Services and Safeguarding Adults pages.

Section 2(1) of the Act states that 'for the purposes of this Act, a person lacks capacity in relation to a matter if at the material time he is unable to make a decision for himself in relation to the matter because of an impairment of, or a disturbance in the functioning of, the mind or brain'.

Section 3(1) states that, for the purposes of section 2, a person is unable to make a decision for himself if he is unable –

(a) to understand the information relevant to the decision,
(b) to retain that information,
(c) to use or weight that information as part of the process of making the decision, or
(d) to communicate his decision (whether by talking, using sign language or any other means).

5d Refusing Consent

If consent to share information can either not be obtained or is refused by a capable adult, the information may still need to be shared to prevent possible future harm to the adult at risk or prevent jeopardy to the assessment / investigation. This will involve weighing up the potential impact of the disclosure, not just in respect of the adult at risk, but also in respect of other individuals who may be affected by the disclosure, against the impact in not disclosing that information. This will be explained to the adult at risk. Where an adult at risk is assessed as having capacity and is refusing to allow disclosure, consideration must be given as to whether their refusal can be over-ridden. A record will be made of the lack of consent and the reasons for exchanging data without it, should the decision be made that the information does need to be shared.

5e Recording Consent

Explicit consent may be given in writing or orally. Written consent is preferable as it reduces the scope for later disputes about the terms of the consent. Consent may also be implicit, for example when a person asks a professional to carry out a task which cannot be done without sharing information.

When consent is given, the professional should ensure that they are clear about the terms of the consent – what information may be shared, and with whom and whether the consent is specifically withheld for sharing particular information or for sharing with a particular agency. The professional should record the consent given and any limits on it and if possible obtain the person's signature on this record. A signed statement should also be obtained if the person gives a blanket or partial refusal.

6. Recording

Clear and accurate records will be kept listing every decision to share information, details of the information shared, with whom and when, and the reasons for this. The record should also include details of the consent approval or refusal.
All requests for anonymity by the referrer will be respected. However, it cannot be guaranteed, especially if the referrer's information becomes an essential element in any subsequent legal proceedings.

7. Framework for Information Sharing

When gathering information for an assessment / investigation or a multi-agency strategy meeting, case conference or review, the following points should always be considered:

- The wishes, if known, of the adult at risk.
- Whether the adult at risk has given consent to involve other agencies.
- The justification for sharing information if consent has been refused. In considering this, the organisations should take regard to the best interests of the adult(s) at risk concerned against the potential implications of non disclosure.
- The impact of assessing the mental capacity of the adult at risk where such an issue is identified.
- the Organisation's internal policies and processes in respect of the disclosure of personal data.
- Whether all the information about the incident/allegations/concerns and the adult at risk is available or whether other information is needed and how it will be gathered. It may be necessary to reconvene the meeting when further information is available.
- Are there any other possible victims, or other people including children who may need protecting?

At the end of any such meeting or information gathering exercise, an agreement should be reached over what information is included within the formal record. There is a standard format for case conference and review minutes. Any information shared in the conference/review forum will be considered strictly confidential and will not be disclosed or discussed with any others unless at any time it is considered to be relevant to the assessment / investigation or necessary to safeguard the adult at risk or any other person.

8. Purposes of Data Sharing

Information may be shared to the following purposes:

Purpose 1: facilitating information gathering and assessment / investigation of an allegation or concern that abuse is taking place and subsequent meetings will be:

- Accurate and up-to-date.
- Relevant to the assessment / investigation.
- To the level of detail required in order to address the identified risks and the purposes of the assessment / investigation.
- Shared on a 'need to know' basis with those agencies identified as providing services relevant to an assessment / investigation or intervention.
- Stored securely within each relevant agency.
- Accessed only by officers and staff with relevant responsibilities.
- Recorded as having been disclosed or not disclosed along with the reason for that decision and who it has been disclosed to.
- Made available to the person to whom the information relates on request, providing there is no risk of harm or prejudice to the assessment / investigation by doing so.
- Retained after the completion of the assessment / investigation according to statutory and local requirements concerning Adult records.

Purpose 2: highlighting or addressing risks to others that may have been identified in the course of an assessment / investigation will be:

- Shared in detail only with those agencies accountable for the reduction or elimination of the identified risk.
- Disclosed to affected individuals and/or their families, but only to an appropriate level of detail.
- Summarised and anonymised before being published or shared in order to highlight more general issues of risk.

Purpose 3: responding effectively to issues of concern which may put adult(s) at risk at risk will be:

- Particular to named individuals identified as potential sources of risk to adults, and, if possible specific to the issue of concern.
- Only to a level of detail required in order to address the identified concern(s).
- Accessed only by officers and staff with relevant responsibilities.
- Disclosed to/shared with a relevant agency only as necessary.

- Stored securely within each relevant agency.
- Recorded as having been shared/disclosed along with the reason for that disclosure and whom it has been disclosed to.
- Made available to the relevant subject on request, providing there is no risk of harm or prejudice to the assessment / investigation by doing so.
- Retained according to statutory requirements.

Purpose 4: monitoring the outcome of assessment / investigations and the effectiveness of services provided will be:

- Summarised and categorised to remove specific detail
- Anonymised wherever possible
- Held securely, with limited access, where detail or personal identification needs to be retained.

9. Legislative Framework for information sharing

Exclusions from non-sharing of personal information are specified in legislation and will take precedence over this information sharing protocol. In particular, Organisations must, in reaching a decision whether or not to share personal data, have regard to:

Data Protection Act 1998

The Data Protection Act 1998 governs the processing of personal data and establishes eight Data Protection Principles which a “Data Controller” such as. The Birmingham Safeguarding Adults Board must observe, either in respect of personal data processed by itself, or where personal data is processed by a third party acting pursuant to the Data Controller’s instructions (a Data Processor).

Personal data means 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, or is likely to come into the possession of, the Data Controller (S.1). For personal data to be lawfully processed, the conditions of Schedule 2 of the Act must be met.

Section 2 states that the following constitutes sensitive personal data with regard to a data subject:

1 racial or ethnic origin
2 political opinions
3 religious beliefs or other beliefs of a similar nature
4 membership of a trade union
5 physical or mental health or condition
6 sexual life
7 the commission or alleged commission by him/her of any offence, or
8 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.

Where information falls within section 2 above, Data Controllers have to satisfy further conditions under the Act for processing to be lawful. In the case of “sensitive personal data”, it is necessary to satisfy one of the conditions in Schedule 2 of the Act and one of the conditions in Schedule 3.

In accordance with the first Data Protection Principle, personal data must be processed “fairly” and “lawfully”, for example, by notifying the data subject why the information is being processed.

Schedule 2 of the Act

Any disclosure of personal data must satisfy one of the conditions in Schedule 2, and in respect of sensitive personal data, at least one of the conditions in schedule 3.

The first condition, in schedule 2, is that the data subject has consented to the disclosure which is also in accordance with guidance on confidentiality published by the NHS and the GMC. If consent cannot be gained for disclosure, one of the other conditions in Schedule 2 must be met for any disclosure of personal data to be lawful.

Schedule 3 of the Act

Any disclosure of sensitive personal data must satisfy one of the conditions in Schedule 3, as well as at least one of the conditions in schedule 2.

The disclosure of medical records, being “sensitive personal data” must also satisfy one of the Conditions in Schedule 3 of the Act. Examples of the conditions in Schedule 3 include:

- Paragraph 1: Where the data subject has given explicit consent to the processing of the personal data.
- Paragraph 3: Where the processing is necessary –
    - In order to protect the vital interests of the data subject or another person, in a case where –
    - Consent cannot be given by or on behalf of the data subject, or
    - The data controller cannot reasonably be expected to obtain the consent of the data subject, or
    - In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- Paragraph 8 (1): Where the data is processed for medical purposes (including the provision of care and treatment and the management of healthcare services).
- Paragraph 6 allows processing where it is necessary in connection with legal proceedings or seeking legal advice.

As with Schedule 2, data controllers are recommended to obtain the patient's consent where possible and consideration should be given to whether it would be practical to obtain consent prior to any disclosure.

Exemptions under the Data Protection Act 1998

Incorporated within the Act are a number of exemptions which allow a Data Controller the ability to disclose personal data without breaching the general presumption not to disclose personal data, as set out in the Act. These exemptions are available in circumstances where the Act recognises that the public interest requires disclosure of personal data .The decision on whether or not to disclose the information on the basis of an exemption is for the Data Controller, but it is recommended that caution is exercised when relying on an exemption, and that a written record of the reasons why a disclosure was made, what evidence was considered when reaching that decision, what exemption was utilised and a copy of the disclosed information, is kept, and that a central register of disclosures is kept.

Section 29 Crime and Taxation

- In accordance with the General Protocol for Information Sharing, West Midlands Police will produce a Form WA170 authorised by a senior officer to support their right to seek information in the investigation of crime. However, information must not be disclosed merely because a form WA170 has been received. Each application is judged on its own merit as to whether the service concerned will consider a release of relevant information, where it, the service, considers that the non disclosure of personal data would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders and/or the assessment or collection of tax.

Section 31 Regulatory activity

- The outcome of the assessment / investigation or safeguarding assessment must be shared with the Care Quality Commission (CQC) where it relates to a regulated service.

Human Rights Act 1998

Article 8 of the European Convention of Human Rights (as incorporated into the Human Rights Act) covers the right of respect for the private and family life of individuals. It states:

- 8(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- 8(2) 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.

Sexual Offences Act 2003

The Home Office has produced guidance entitled “Adults: Safer from Sexual Crime” on the exchange of information about those who have been convicted of, cautioned for, or otherwise dealt with by the courts for a sexual offence, and those who are considered by the relevant agencies to present a risk to children and others. The guidance also addresses issues in relation to people who have not been convicted or cautioned, but who are suspected of involvement in criminal sexual activity.

Multi-Agency Public Protection Arrangements (MAPPA)

Violent and sexual offenders are supervised by police, probation, youth offending teams and mental health services. These organisations can refer offenders for consideration by a multi-agency meeting. The task of these meetings is to share information, assess the risk(s) the offender represents, and plan safeguards to protect the public. Every case has built-in timescales for the risk management plan, individual accountability and a mechanism for checking progress. MAPPA are set up in Birmingham to consider the risks posed by sexual and violent offenders. Sharing of information through MAPPA must be approved by the Chief Constable.

Joint memorandum of understanding between NHS, ACPO and HSE (Feb’06)

“NHS bodies have a responsibility amongst other things to ensure the safety and well-being of patients and to investigate when things go wrong. NHS organisations must conform to national and local policies and procedures in discharging this responsibility.”

NHS Code of Confidentiality 2003

This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients’ consent to the use of their health records and should be referred to where informed consent has not been provided by the patient/ adult at risk.

The Code:

1 introduces the concept of confidentiality;
2 describes what a confidential service should look like;
3 provides a high level description of the main legal requirements;
4 recommends a generic decision support tool for sharing/disclosing

information;
5 lists examples of particular information disclosure scenarios.

The Code can be found at: www.doh.gov.uk.

Freedom of Information Act 2000

FOIA enables written requests for recorded information to be processed and documents released, subject to some absolute and qualified exemptions, with a Public Interest Test applied where necessary. This Information Sharing Protocol will be included in the FOI Publication Scheme of the relevant agencies and will be eligible for release on request. However, Personal data will generally be exempt from disclosure under the Freedom of Information Act

Police Act 1997

There may be a statutory obligation on the participating organisations not to disclose information given to assessment / investigation meetings by the police.
Such a situation should be made clear at the beginning of any safeguarding meeting.

Other Legislation which may affect information sharing:

Mental Capacity Act 2005

The Act came into force on a phased basis during 2007. It is intended to enable and support people aged 16 or over who lack capacity to make decisions, not to restrict or control their lives. The Act aims to protect people who lack capacity but also to maximise their autonomy and ability to participate in decision-making.

Sections 2 and 3 (outlined above) outline the test for capacity.

Section 4 places a duty on people making decisions about a person who lacks capacity to act in that person's best interests. It also provides a checklist to assist in making a decision in a person's best interests, including:

- considering all relevant circumstances including whether the person will likely regain capacity (and when that may be). "Relevant circumstances" are those which the decision maker is aware of and are considered relevant.
- A decision maker must take into account, if it is practicable and appropriate to consult them, the views of the following people with regard to what would be in the person's best interests –
- Anyone named by the person as someone to be consulted on the matter in question or on matters of that kind
- Anyone engaged in caring for the person or interested in his welfare
- Any donee of a lasting power of attorney granted by the person, and
- Any deputy appointed for the person by the court
- consider, so far as is reasonably ascertainable –

- the person's past and present wishes and feelings (and, in particular, any relevant written statement made by him when he had capacity),
- the beliefs and values that would be likely to influence his decision if he had capacity, and
- the other factors that he would be likely to consider if he were able to do so

Section 44 of the Act makes it clear that where somebody cares, is an attorney under a Lasting Power of Attorney or Enduring Power of Attorney for a person who lacks capacity, they will commit an offence if they ill-treat or wilfully neglect the person.

Crime and Disorder Act 1998

The key areas of the Act were the introduction of Anti-Social Behaviour Orders, Sex Offender Orders, Parenting Orders, gave local authorities more responsibilities with regards to strategies for reducing crime and disorder, and the introduction law specific to 'racially aggravated' offences.

Each Local Authority in the country was given the responsibility to formulate a strategy to reduce crime and disorder in their area. The act also required the authorities to work with every police authority, probation authority, health authority and any body/person prescribed at that time by the Secretary of State.

10. The Partner Agencies subject to this protocol are:

Birmingham City Council

Birmingham Community Healthcare NHS Trust

NHS England Birmingham, Solihull and the Black Country

Birmingham Cross City CCG

Birmingham South Central CCG

Sandwell and West Birmingham CCG

Birmingham and Solihull Mental Health NHS Foundation Trust

Heart of England NHS Foundation Trust

Sandwell and West Birmingham Hospitals NHS Trust

University Hospital Birmingham NHS Foundation Trust

Birmingham Women's NHS Foundation Trust

Royal Orthopaedic Hospital NHS Foundation Trust

West Midlands Police

Staffordshire and West Midlands Probation Trust

Care Quality Commission

Service Birmingham

West Midlands Fire Service

West Midlands Ambulance Service

Voluntary organisations involved in cases

Private Healthcare Providers

Contracted providers of Social Care services

Contracted providers of Supported Housing facilities

The requirement to comply with this information sharing protocol will be incorporated in a safeguarding adults clause to be included in all relevant contracts or service level agreements between the Partner Agencies and their relevant service providers.

11. Implementation, Monitoring and Review

This document has been developed to provide a purpose-specific protocol to support the Safeguarding procedure. It adopts the principles and standards set out in the overarching "General Protocol for Sharing Information between the Birmingham Health Community and Social Care and Health" (February 2004) as a base line. This protocol sets out the specific arrangements and responsibilities for sharing information relating to adult(s) at risk.

This protocol will normally be reviewed on an annual basis, taking any changes in practice, relevant legislation or organisational structure into account. Issues, incidents and complaints resulting from failures in the specific agreements will be fed into the review processes.

In the event of a requirement for an urgent change to this protocol, upon agreement of all the parties, an urgent review of the procedures requiring a change will be undertaken.

Breaches of this protocol will be seen as a matter of serious concern and partner agencies will take immediate action should such any such breach occur.

Partner agencies may find it useful to produce an internal Procedure within their own organisation to outline for their staff how the protocol should be operated in day-to-day practice on a 24 / 7 basis. Such a third tier document should be seen as

supplementing this Protocol

12. Security in Information Transfer

The personal data items included in the Information Sharing Protocol for Safeguarding Adults should always be treated securely and confidentially.

Transfer of the information within organisations and between organisations should be subject to the terms and guidance of the Data Protection Act 1998 principle 7 on security and to the procedures, codes of practice, standards and policies of the organisations concerned.

Personal data includes any information that can be used to identify an individual and transferring data means sending personal data electronically to anyone outside the organisation, sending data by post or physically taking data from one building to another, or to another organisation, or even the disclosure of personal data in a conversation, either during a face to face meeting or over the telephone.

Transferring means using both manual and electronic methods of providing information to someone inside or outside the organisation. This includes:

- copying data on to CDs
- copying data on to memory sticks and flash drives
- taking data away on a laptop
- attaching a file of data to an e-mail message
- uploading a file to another computer system
- printing out data on paper and sending or taking it from the office.

Any sharing of personal data should be made in accordance with the disclosing Organisation's internal data security / data protection policies, procedures and standards, having due regard to the sensitivity of the information and the appropriate method of transfer.

All data should be assessed and a security level assigned to it. The security level should be written or typed clearly on the data e.g. RESTRICTED.

The degree of security that should be applied is then determined by that security level.

The minimum expectation is that:

- personal data that is kept in an electronic format on any portable devices (e.g. laptop, PDA, blackberry, etc) or portable media (.e.g CD, DVD, USB Memory stick or portable hard drive) should be kept in an encrypted and password-protected format and the password/encryption key should not be stored on or with the device or media, and that any such personal data should only be information necessary for the specific purpose and should not be excessive.

Personal data which is at significant risk should be encrypted before being transferred.

Examples of significant risk are:

- data kept on a laptop, Blackberry or PDA, which might be stolen
- data copied on to a memory stick, flash drive or CD, which might easily be stolen or mislaid
- a file attached to an e-mail message which is sent to someone outside the organisation.

Upon receipt of the shared information, the recipient body is deemed to be a Data Controller in its own right in respect of that shared data, and is therefore legally responsible, under the Data Protection Act, for that data in its possession or control.

13. Breach management

In the event of any party to this protocol becoming aware or having a reasonable suspicion that a breach of the Data Protection Act , i.e. that unauthorised disclosure, loss or destruction of personal data has occurred in respect of the Data processed under this Data Processing Agreement, it shall notify:-

the other parties to the protocol involved in relation to the Data Subject(s) affected or likely to be affected by the actual or suspected breach;

as soon as possible and no later then 2 working days after becoming aware or having a reasonable suspicion that a breach has occurred.

As soon as a notification has been made, the parties involved must liaise to determine what steps, if any, can be taken to

a) determine whether or not the Data Subject or their legal representative should be notified of the breach.
b) mitigate any impact of the breach in relation to the individuals who may suffer harm from the breach,
c) investigate the actual or suspected breach; and
d) take steps to prevent a re-occurrence of the breach. ,

The decision to report any breach will be made under either:-

In respect of NHS organisations, the Health & Social Care Information Centre Checklist Guidance;

In respect of non NHS organisations, the Notification of data security breaches to the Information Commissioner's Office (ICO) guidance document.

Sub-Appendix 1

Information which may be shared under the Safeguarding Adults process

- The names, dates of birth and other personal details of the alleged victim of abuse or neglect
- Details of the person making the referral or reporting the incident
- Details of alleged incident(s)
- Names and contact details of witnesses (where appropriate)
- Names, status and contact details of the alleged victim's relatives or carers
- Details of alleged victim's health and needs
- Details of the alleged victim's financial status (where appropriate)
- Details of the alleged victim's support network
- Details of the alleged victim's capacity
- Details of any professional or voluntary workers involved in the care provision to the alleged victim
- The names, dates of birth and other personal details relating to alleged perpetrator(s) of abuse or neglect
- Details of the alleged perpetrator's financial status (where appropriate)
- Details of the alleged perpetrator's capacity
- Details of any other worker in any organisation who may have information relevant to the assessment / investigation of the incident

These data are not exclusive and may change depending on individual cases and circumstances.

Please note that national guidelines on the Safeguarding Adults Dataset may affect the amount of information held and shared by organisations in individual cases and aggregated for monitoring purposes.

Sub-Appendix 2

The General Protocol for Sharing Information: Summary

The Protocol sets out standards and principles to be applied whenever personal information is shared or exchanged. All the organisations signed up to the Protocol are fully committed to ensuring that these standards and principles are adhered to at all times.

Organisations and agencies in Birmingham recognise that initiatives requiring a multi-agency approach cannot be achieved without the exchange of information about individual service users, levels of activity, the level and nature of resources and about their approach to addressing the issues. Their agreement to develop multi-agency working therefore includes a commitment to enable such information to be shared in ways that are compliant with their statutory responsibilities and the requirements of the law.

- Information about individuals will only be shared when and where it is needed.
- Information will be shared in accordance with statutory duties.
- Information that is provided in confidence will be treated as confidential.
- Information will only be used for the purposes for which it was collected and shared.
- Individuals will be fully informed about the way their personal information is used and shared.
- Consent to share information will always be sought from the appropriate individual.
- Considerations of confidentiality and privacy will not automatically cease on death.

In observing the Data Protection Act (1998), signatories will work to ensure that the following principles apply in handling personal information:

- where there is a choice as to whether the information can be shared or not, it will be as easy as possible for an individual to exercise that choice;
- information will only be processed without an individual's knowledge where this is assessed by the data controller as necessary for purposes such as national security, public safety, statistical analysis, the protection of the economy, the prevention of crime or disorder, the protection of health or morals, or the protection of the rights and freedoms of others;
- only information which is actually needed will be collected and processed; - personal information will only be seen by staff who need it to do their jobs;
- any information which is no longer needed will be deleted;
- decisions affecting an individual will only be made on the basis of reliable and up to date information;
- personal information will be protected from unauthorised or accidental disclosure;

- subject to any statutory exemptions, a copy of any information held will normally be provided on request;
- any inaccurate or misleading information will be checked and corrected as soon as it is identified; and
- proper procedures will be in place for dealing promptly with any complaints that are made.

The principles apply to personal information which is held both on computer and in some paper records (including all papers records previously covered by the Access to Personal Files Act1987).

Service-specific Data Protection Statements

Wherever personal information is collected, the agency responsible will publish a Data Protection Statement for that service which will set out clearly:

- who will see it;
- why they need it;
- what they will do with it; and
- when they will delete it.

They will also state:

- how that personal information is safeguarded;
- how an individual can check and correct the information that is being held;
- how to pursue a query or complaint; and
- where to get more information.

The detailed version of this Protocol is also available.

Sub-Appendix 3

Adults and Communities Directorate Confidentiality Code of Conduct

This DRAFT Code of Conduct applies to all people who have access to personal information held in any Directorate manual or IT system (Service Birmingham staff, partner organisation staff, agency staff, volunteers, students, etc).

All such people are responsible for ensuring that personal information gained in the course of duty is not disclosed to any person or organisation who does not need to know or who does not have an authorised right of access to that information.

Confidentiality must be maintained. All such people should safeguard personal information by following the basic rules listed below.

- **disclose information only to people authorised to receive it** – this includes staff directly involved in the assessment and care of the person
- **do not divulge your computer or security passwords to any other person** – If you suspect someone knows your password then you must change it
- **do not use someone else's user ID or password to gain access to information**
- **do not leave a computer terminal logged onto the system unattended**
- **do not take personal records out of the office unless necessary.**
- **do not leave personal records unattended**, especially in public areas. Printed material containing personal information should not be left unattended on printers or fax machines.
- **do not download personal information from the directorate's systems onto another computer system** without permission from the data controller
- **take care not to disclose personal information inadvertently** - if you can be overheard in a public place: keep your voice down; in reception do not ask for personal information if possible; use an interview room if possible
- **all information must be, to the best of your knowledge, accurate and up-to-date**
- **do not access information about yourself, your relatives or friends** – You do not have an automatic right to such information. If you recognise that you are accessing information about someone you know in the course of carrying out your duties you must declare this to a manager and arrangements should be made for another colleague to complete the work.
- **only give confidential information over the 'phone or via fax** after first checking the identity and authority of the caller/receiver
- **confidential service user files should be kept securely** in locked files
- **emails about service users** should be treated as confidential and sent with appropriate confidential identification
- **essential e-mail attachments** about service users should be sent using encryption where available
- **confidential waste should be shredded or put into a confidential waste bag** - do not use as scrap paper

- **confidential waste should always be stored securely while waiting for disposal**
- **confidential waste should always be disposed of in a secure manner**
- **make yourself aware of your office procedure for mail and adopt a practice which would ensure that personal information is kept confidential,** ensuring the address on any envelope is correct and clearly written
- **finally, seek advice when you need it** and refer to related directorate policies

Sub-Appendix 4

Acknowledgements

This document has been developed in line with recognised good practice and draws on documents and work already undertaken to address these issues in Birmingham and in other areas of the country.

These documents include:

- The Data Protection Act 1998 and associated Guidance from the Office of the Information Commissioner
- The Crime and Disorder Act 1998
- The Human Rights Act 1998
- NHS Code of Confidentiality 2003
- The Caldicott Manual – Guidance for Guardians
- Department of Health Guidance on the Development of Information Sharing protocols
- Birmingham Safeguarding Committees – Multi-Agency Guidelines – Protecting adult at risks [June 2005]
- Birmingham City Council – Adults and Communities – Safeguarding Policy, Procedure and Good Practice Guide
- Care Quality Commission – Our Safeguarding Protocol and Code of Practice on confidential personal information
- ADASS [Association of Directors of Adult Social Services] – Protocol for inter-agency assessment / investigation of adult at risk abuse
- Birmingham Safeguarding Children's Board – information sharing guide
- North East Lincolnshire Inter-agency Policy documents on Sharing Information
- Safeguarding Adults: A National Framework of Standards for good practice and outcomes in adult protection work", ADASS, October 2005
- No Secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse" Dept. of Health, March 2000
- Safeguarding adults: multi-agency policy and procedures for the West Midlands July 2012

Additional reference documents:

- The Information Governance Review (March 2013).
- Caldicott Information: To Share or note to share. Government Response to the Caldicott Review (September 2013)
- A guide to confidentiality in health and social care (September 2013). HSCIC