

Berkshire Safeguarding Adults Boards' Information Sharing Protocol

May 2019

Berkshire Safeguarding Adults Boards' Information Sharing Protocol



Version Control

Author	Date	Version	Comments
V Nosal	30/05/2019	1	Signed off by Berkshire SAB's June 2019

There is a dedicated website for Safeguarding Adults Policies and Procedures which can be found here:
<https://www.berkshiresafeguardingadults.co.uk/>

If you have any queries please discuss with your manager you can contact the Policies and Procedures Subgroup directly about the content of this framework by completing a request for amendments form which can be found on the Berkshires Policies and Procedures Website:
<https://www.berkshiresafeguardingadults.co.uk/>

Berkshire Safeguarding Adults Boards' Information Sharing Protocol

This Protocol has been adopted by the Safeguarding Adults Boards for the West of Berkshire, Bracknell Forest and Windsor & Maidenhead and Slough. It covers all of the agencies that form the West of Berkshire Board in the three unitary authority areas of Reading, Wokingham and West Berkshire. It provides a framework for ensuring that the making of decisions regarding sharing information about vulnerable adults who may be at risk of abuse or neglect is conducted within statute and regulatory guidance.

The Protocol offers guidance to front-line staff in assessing possible risk to adults, and in balancing the risk against the rights to confidentiality and privacy of those who may be a source of risk.

The key stages in the procedure set out in the Protocol are to:

- assess the risk a person is thought to be exposed to or may pose to others;
- decide which (if any) agencies or individuals need to be told, and what they need to know;
- consult the person who may be exposed to risk and those who may be causing concern; and (if appropriate)
- Share the information in compliance with this Information Sharing Protocol and Central Government's 7 Golden Principles of Information Sharing.

1 INTRODUCTION

PARTIES

1.1 This Protocol is adopted by the Safeguarding Adults Boards for the West of Berkshire, Bracknell Forest and Windsor & Maidenhead and Slough. The composition of each Board is slightly different depending on local need.

PURPOSE

1.2 The purposes of this Protocol are:-

- a) **to promote** the safeguarding of adults by the carefully considered sharing of information about identified risks, and



- b) **To help** front-line staff fairly and consistently to balance the risks of non-disclosure against the infringement of individuals' rights to privacy and confidentiality.

STATUS

1.3 This Protocol comprises local policy and procedure for inter-agency work to safeguard vulnerable adults within the national framework provided by the law, and Departmental and other guidance – see sections 42 to 45 of the Care Act 2014 and, in the Care and Support Statutory Guidance ¹ paras. 3.47 – 3.48 and chapter 14 on pages 189 – 224.

1.4 This Protocol should be read together with any individual agency procedure governing information sharing to safeguard vulnerable adults. Any conflict between local procedures and this Protocol should be discussed with a senior manager within the Agency concerned and a legal adviser; it should also be reported for information to the Safeguarding Adults Board.

SCOPE

1.5 This Protocol only covers inter-agency sharing of information for purposes of safeguarding adults. In particular, it does not cover information-sharing or disclosure which is addressed in the following:-

- a) for disclosure between Social Care, Police and Crown Prosecution Service, the Thames Valley Disclosure Protocol ²;
- b) for patient- or service-user access to records, the Access to Records policy of the Agency concerned;
- c) for information-sharing or disclosure in connection with the Multi-Agency Public Protection Panel, the Panel's information-sharing or disclosure arrangements under MAPPA Guidance issued by the Ministry of Justice ³;
- d) For information-sharing in connection with a Multi-Agency Risk Assessment Conference (MARAC), any protocol adopted by member agencies.

¹ Department of Health February 2018 - [Care Act statutory guidance](#)

² Copies obtainable from the Joint Legal Team, 0118 937 2986. See also the (national) 2013 [Protocol](#) and Good Practice Model - Disclosure of information in cases of alleged child abuse and linked criminal and care directions hearings (October 2013).

³ <http://www.justice.gov.uk/downloads/offenders/mappa/mappa-guidance-2012-part1.pdf>



PRINCIPLES

1.6 Upholding the principles of the GDPR (Appendix 1) will constitute the main focus of this document however the secondary principles underpinning this Protocol are as follows:-

- a) selective disclosure of information is crucial to the inter-agency and inter-disciplinary processes of assessing and addressing risks to adults;
- b) confidential information will not be shared unless there is a clearly articulated case for doing so, based on the individual case and situation;
- c) Information-sharing is not an end in itself, but can be a crucial component of a successful, comprehensive safeguarding plan.

GUIDANCE FROM KEY PROFESSIONAL BODIES ON INFORMATION-SHARING

- [NHS England's Confidentiality Policy](#)
- [Health and Care Professions Council's Guidance on Confidentiality](#)
- [Nursing and Midwifery Council's Code for nurses and midwives](#)
- [CQC Code of Practice on confidential personal information](#)

2 OVERVIEW OF THE LAW

*This is an outline of the law governing the sharing of confidential information.
It is important to seek specific advice in the context of individual situations.*

CONFIDENTIALITY AND PRIVACY

2.1 Organisations holding personal information are under a common law duty of confidentiality which governs the way the information may be stored and disseminated. In addition, individuals have rights under the Human Rights Act 1998 and European Convention on Human Rights.

GENERAL DATA PROTECTION REGULATION (GDPR)

2.2 The GDPR was implemented on 25 May 2018. Agencies are fully committed to ensuring that if they share information it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of the EU General Data Protection Regulations ("GDPR"), and the Data Protection Bill 2018 (**together "Data Protection Legislation"**). The Agencies will also take into



consideration any guidance issued by the Information Commissioners Office; the Human Rights Act 1998; the Common Law Duty of Confidence.

2.3 The Authorities must have (and by signature of this ISA confirm that they do have) in place policies and procedures to meet the national requirements for

- a) Data Protection,
- b) Information Security and
- c) Confidentiality.

2.4 Implementation of GDPR means that where disclosure is reasonably necessary to fulfil a statutory duty it is permitted. This includes the sharing of information about risk to an adult in the context of assessment under the Mental Health Act 1983 or the Care Act 2014.

INFORMATION FOR DATA SUBJECTS

2.5 GDPR requires that data subjects are informed before the sharing of their sharing personal or special categories (see article 9 appendix 3) data with the Agency and that data sharing will be performed to ensure the best care can be provided. [General Data Protection Regulation \(EU\) 2016/679](#)

The Agency relies on the GDPR Article 6(1) (c) and (d) (see appendix 2)

GDPR AND DISCLOSURE

2.6 Where a data subject lacks capacity to understand the obligations under GDPR, an assessment has to be made as to whether disclosure is “reasonable in all the circumstances”. This assessment should take into account:-

- a) any duty of confidentiality owed to the data subject;
- b) the steps taken to advise the data subject about Board’s legal obligations; and whether the data subject is capable of understanding the Boards legal obligations under the GDPR

If at the initial point of contact the data subject or their representative/carer does not agree to their personal or special categories data being shared the Board understands that the service provided to the data subject may be restricted.



CRIME AND DISORDER ACT

2.7 Section 115 of the Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act 1998 contains a general power for anyone to disclose information to Social Services, Probation, the Police or Health. Such disclosure has to be “necessary or expedient” for one of the purposes set out in the Crime and Disorder Act, which include “preventing or reducing crime”. This power goes in tandem with the duty under the Data Protection Legislation to seek consent to disclosure if possible.

CASE LAW

2.8 The courts have also made clear that disclosure based on sufficient evidence and a specific risk assessment is permitted. In the North Wales case⁴, the Court of Appeal held that it was lawful for the police to disclose information about a person’s convictions and history where they were assessed as posing a considerable risk to children and vulnerable adults. Disclosure should however only be made where there was a “**pressing need**” for it. The Court also considered that it would be important to forewarn people of the gist of the information held about them, and to give them the opportunity to comment before any information is shared.

2.9 On the other hand, in R (A) v National Probation Service (2003)⁵ the High Court held that the Probation Service were not entitled to inform the landlord of someone about to be released from prison (Mr A) that he had been convicted six years before of murdering his wife. Instead of addressing risk posed by Mr A to others and deciding if this warranted the exceptional step of disclosure, the Probation Service had assumed that the conviction should be disclosed unless there was reason not to.

2.10 The case of A Local Authority v SK & HK⁶ concerned proposed information-sharing with a care home for older people, one of whose staff had been found to have seriously and repeatedly assaulted her 8-year-old daughter. The mother denied responsibility and even forged a confession from a friend, whom the judge found did not exist. The court gave permission for this information to be disclosed to the care home and the local authority for the area. The judge stressed the links between abuse of adults and of children:-

“ ... the standards to be expected of those looking after children may be no less than those looking after vulnerable adults.”

⁴ R v Chief Constable of North Wales Police ex parte Thorpe [1998] 2 FLR 571.

⁵ [2003] EWHC 2910 (Admin)

⁶ [2007] EWHC 1250 (Fam) Sumner J.



HUMAN RIGHTS

2.11 In addition to the rights to have information about them treated confidentially, individuals have the right to respect for their private and family life under Article 8 of the European Convention on Human Rights. Any disclosure of personal information is required to be “proportionate” to the risk involved and “necessary ... for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”. The “rights and freedoms of others” would include the rights of others, including children and vulnerable adults under Article 3 of the Convention not to “be subjected to inhuman or degrading treatment ...”, which is likely to include most if not all forms of abuse and neglect.

2.10 Potential victims and those giving rise to concern also have the right under Article 6 to be given a “fair hearing”. This includes being kept informed, having their views recorded and considered, and being given a reasoned explanation of any decision about disclosure.

KEY LEGAL POINTS

- 1. The disclosure of personal information should be “the exception not the rule”⁷.**
- 2. The GDPR and associated guidance from the Information Commissioner’s Office [ICO] should be the reference point to ensuring that disclosure is lawfully and fairly completed and that the data subject is advised at the initial point of contact how their personal and/or special categories data will be used. The Board advocates that they will comply with the Data Protection Legislation where the data subject lacks capacity to understand the legal obligations of data sharing, in order that a child or vulnerable adult is not at risk of significant harm.**
- 3. Personal information should only be disclosed where there is a “pressing need” to do so. Deciding whether there is a pressing need to disclose will depend on properly balancing the infringement of the individual’s rights to privacy and confidentiality against the assessed risk and the extent to which disclosure is likely to help reduce that risk.**

⁷ Exparte LM [2000] 1 FLR 612 at 622C.

3 DISCLOSURE OF INFORMATION IN INDIVIDUAL CASES

APPROACH TO DISCLOSURE

3.1 The process of deciding whether to disclose confidential information will involve the following steps:-

- a) deciding the likely nature and degree of risk posed;
- b) deciding if this risk (and / or a duty on the part of the holder of the information or the proposed recipient) suggests a need to disclose;
- c) deciding if there is sufficient reason not to seek consent, and seeking any that is considered necessary; and
- d) if consent is refused or no response is received, then a decision regarding public interest, harm to data subject and/or other individuals and whether a crime has/is likely to be committed will guide the decision to share information. If the decision is made to share then the data subject should be informed unless to do so would result in the risk of serious harm for themselves and others or, where a crime investigation may be jeopardised.

3.2 These decisions will be made in accordance with the principles set out at para. 1.6 Above.

3.3 Decisions will be recorded by the agency holding the information, with reasons.

FACTORS IN RISK ASSESSMENT

3.4 The source, degree and type of risk should be spelled out using the following risk factors:-

- a) Any convictions or cautions against adults or children, particularly for violence
- b) Any civil court findings that the person (may have) perpetrated abuse in the past and / or posed an unacceptable degree of risk⁸

⁸ It is important to note that the findings of courts sitting in private should not be disclosed to non-parties without the court's permission: see Re V & L [1999] 1 FLR 267.



- c) The professional view (at the time, or since) of the plausibility of any serious allegations which did not result in convictions or court findings
- d) The passage of time since any convictions, findings or plausible incidents
- e) Any therapy undergone, and outcome if known
- f) The level of risk indicated by any risk assessment carried out in the past
- g) The subject's attitude towards past convictions, findings and plausible incidents – degree of insight, empathy towards victims, awareness of triggers to abuse
- h) Extent of contact the subject is likely to have with vulnerable adults, unsupervised in particular, and
- i) The capacity of carers or others to protect adults who may be at risk.

DISCLOSURE
AFTER
CONSULTING

3.5 The person giving rise to the concern should usually be forewarned of the substance of the allegations against them and invited to comment before disclosure takes place. Such consultation should only be omitted in cases of serious, urgent risk where delay (or forewarning) will cause unacceptable risk. In such cases, the person should be informed after disclosure unless (very exceptionally) there is evidence that informing them even after the event will cause unacceptable risk.

EXPLAINING
DECISIONS

3.6 The reasons underlying any decision to disclose or not to disclose information under this protocol should be carefully recorded, and communicated to those who have been consulted prior to disclosure. Lay recipients should be reminded that the information is confidential and should be informed of the reasons for disclosure to themselves. Decisions to refuse disclosure requests should also be explained.

3.7 The range of decisions on disclosure is illustrated in the table below.



<u>Disclosure decision</u>	<u>Rationale for disclosing (or not)</u>	<u>Rationale in relation to consultation / consent</u>
No disclosure	Disclosure not considered necessary for assessment of needs and risks to adults	Consultation and compliance to Data Protection Legislation does not arise
Disclosure	Disclosure likely to be helpful in assessing needs and risks BUT ... ➔	Risks do not justify overriding confidentiality
Disclosure on notice	Disclosure necessary to safeguard adults	Data Subject has opportunity to a) comment on concerns and b) take advice prior to disclosure
Disclosure followed by informing the subject	Disclosure urgently needed to avert risk to adults	Urgency precludes consultation
Disclosure without informing the subject at any point	Disclosure urgently needed to avert risk to adults, AND ... ➔	Informing the subject is likely to cause unacceptable risk



APPENDICES (see ICO [“The Principles”](#))

Appendix 1

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').



Appendix 2

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.



Appendix 3

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis



of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.