**Berkshire Safeguarding Adults’ Information Sharing Protocol**

**Version History**

| **Version** | **Date** | **Date Endorsed by:** | **Description**  |
| --- | --- | --- | --- |
| 0.15 | 18/08/25 | Berkshire Policy and Procedure Subgroup: DRAFT | DRAFT |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Contents**

[1. The Purpose of this Protocol 3](#_Toc202870768)

[2 Confidentiality 4](#_Toc202870769)

[4 Consent to Share Information 6](#_Toc202870770)

[5 Consent and Mental Capacity 7](#_Toc202870771)

[6 Data Protection/Liaison Officers 7](#_Toc202870772)

[7 Raising concerns and whistleblowing 7](#_Toc202870773)

[8 Keeping data safe: exchange storage and retention 8](#_Toc202870774)

[9 Security 8](#_Toc202870775)

[10 Individual Responsibilities 8](#_Toc202870776)

[11 Information sharing with regards to Safeguarding Adult Reviews 9](#_Toc202870777)

1. **The Purpose of this Protocol**
	1. This protocol forms the basis for ensuring best practice around the lawful exchange of information between organisations working with adults with care and support needs (referred to as “the adult”) in Berkshire. This includes the exchange of information through adult safeguarding, and intervention mechanisms such as MARM (Multi-Agency Risk Management Framework), MARF (Multi-Agency Risk Framework) or MART (Multi-Agency Risk Tool) platforms, or under s.44 of the Care Act.
	2. This protocol should be read in conjunction with existing information sharing agreements between agencies, and all agencies must continue to follow those relevant local agreements when dealing with specific issues.
	3. Partner Organisations
* Bracknell Forest Borough Council
* Reading Borough Council
* Royal Borough of Windsor & Maidenhead Council
* Slough Borough Council
* West Berkshire Council
* Wokingham Borough Council
* Thames Valley Police
* BOB Integrated Care Board
* Frimley Integrated Care Board
* NHS England
* Berkshire Healthcare Foundation Trust
* Royal Berkshire Hospital Foundation Trust
* South Central Ambulance Services
* National Probation Service
* Royal Berkshire Fire and Rescue Service
* Organisations involved with adults with care and support needs in Berkshire
	1. By becoming a partner to this protocol, Partner Organisations are making a commitment to apply the Information Commissioner’s Code of Practice’s ‘Fair Processing’ and ‘Best Practices’ Standards and adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).
	2. This protocol is not legally binding but is to be used to set good practice standards that the Partner Organisations need to meet in order to comply with relevant legal duties in relation to the sharing of personal information.
	3. The protocol applies to all staff employed by the organisations: permanent or temporary, consultants, casual, agency workers and any volunteers.
	4. It refers to all and any information held on a computer system (in the cloud or hard drive) or on paper including personal data and sensitive personal data as defined in the DPA and the UK GDPR. Partner organisations are expected to have their own protocols to cover the requirements as to how data may be stored or transported, by email or otherwise. It is required that all partner organisations adhere to their existing policies in place about how information can be shared and how documents must be marked.
	5. There are existing legal requirements and protocols in place which cover when information should be shared between other organisations and the police in the event of an ongoing criminal investigation or trial. This protocol does not override those existing arrangements. However, there may be emergency situations in the context of safeguarding under the Care Act, when police require information immediately, in which case this protocol will apply with regards to providing the information needed to address that emergency.
	6. This protocol covers:
		+ confidentiality
		+ reasons for sharing information
		+ consent and when it is unnecessary or inappropriate to secure it
		+ data protection and liaison officers
		+ security
		+ raising concerns about internal processes: “whistleblowing”
		+ keeping data safe: exchange storage and retention
1. **Confidentiality**
	1. Information (data) which is either “personal” or ”special category[[1]](#footnote-2)“ data is subject to a duty of confidentiality. This means that it should only be shared for a specific lawful purpose or where appropriate consent has been obtained.
	2. “Personal data” is about an identifiable adult. The adult can be identified from the information either by name or by association, because of the content of the information itself.
	3. “Special category data” consists of the following information about an adult: their racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, data concerning a person’s sex life and their sexual orientation. This information is afforded particular protection and careful consideration should be given before sharing it.
	4. There may be occasions when it is inappropriate to share information that does not specifically identify an individual, but it is treated as confidential for other reasons. These could include because it is commercially sensitive, or because of a separate agreement or contract requiring confidentiality. This type of information is not covered by this protocol and advice should be sought if this is a genuine concern.
2. **Reasons for sharing information**
	1. No professional should assume that someone else will pass on information and as a consequence refrain from doing so, when they judge that the information may be critical for the safety or wellbeing of an adult.
	2. Sharing information appropriately between organisations is part of day-to-day safeguarding practice: organisations need to share safeguarding information with the right people at the right time to provide co-ordinated input to adults with care and support needs who are at risk of abuse or neglect, whilst also considering the prevention of abuse or neglect.
	3. Information can only be shared for the following purposes:
		* promote well-being
		* prevent death or serious harm
		* coordinate effective and efficient responses to assessed need
		* enable early interventions to prevent the escalation of risk of harm
		* prevent abuse and harm that may increase the need for care and support
		* maintain and improve good practice in safeguarding adults, reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
		* identify low-level concerns that may reveal people at risk of abuse
		* help people to access the right kind of support to reduce risk and promote wellbeing
		* help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
		* reduce organisational risk and protect reputation
	4. Appropriate information sharing is essential to provide a coordinated response in respect of adults with care and support needs who may be at risk or experiencing abuse and neglect irrespective of whether they are receiving care and support or not. Any information should be shared on a “need to know” basis and with a view to being:
		* under the statutory obligations to investigate the risk to adults with care and support needs set out in the Care Act 2014
		* is in the interests of the Data Subject e.g. in relation to their health
		* in the public interest to prevent harm to others
	5. The [seven golden rules](https://www.england.nhs.uk/long-read/safeguarding/) of information sharing are:
		* the DPA, UK GDPR and other legislation are not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
		* be open and honest with the person from the outset about why what and how and with whom information will be shared or could be shared and seek their agreement, unless it is unsafe or inappropriate to do so (see below re consent)
		* seek advice where appropriate
		* share with consent where appropriate and where possible respect the wishes of those whom do not consent to share confidential information (see below re consent)
		* consider safety and wellbeing – base your information sharing decision on considerations of the safety and well- being of the person and others who may be affected by their actions
		* necessary, proportionate, relevant, accurate timely and secure ensure that the information which you share is necessary for the purpose which you are sharing it, shared only with those organisations who need to have it, accurate up to date and shared in a timely fashion
		* information should be shared for a particular purpose. It should not be forwarded on, (even to another organisation) without careful consideration that it is appropriate to do so. There may be a reason why information should not be disseminated further (Checks must be made with the source of the information, the data controller, and prior to forwarding on information, save in an emergency)
3. **Consent to Share Information**
	1. The starting point must always be to seek the informed consent of the adult before sharing information with other services or organisations. Consent should be obtained wherever possible, unless there are clear and lawful reasons not to do so: such as where the individual lacks mental capacity, or where seeking consent would place them or others at risk of serious harm. However, information can still be shared without consent if it is not possible to obtain it, or if consent is declined, provided there is a legal basis to do so. This may include situations where there is a risk of abuse or neglect, or where it is necessary to protect the vital interests of the individual or others.
	2. Organisations involved with adults with care and support need process data mostly under the public task and legal obligation lawful bases as the duty of confidentiality is not absolute and, in most cases, where it is appropriate to share information, obtaining consent wouldn’t matter as data will be shared regardless if safeguarding is triggered.
	3. However, the factors listed below should be considered before a decision is made to share information. It is a balancing exercise: whether the requirement for information for confidentiality should be overridden by the reason that it is considered necessary to disclose. In situations of doubt, specialist or legal advice should be sought.
	4. All information is shared in confidence and the rules of confidentiality always apply.
	5. Partner organisations can share information even when consent is refused. This is because their lawful bases in those instances include the following:
		* **contract** – necessary for a contract partner organisations have with the individual, or because they have asked you to take specific steps before entering into a contract
		* **legal obligation** – necessary for the partner organisation to comply with the law (not including contractual obligations)
		* **vital interests** – necessary to protect someone’s Iife
		* **public task** – necessary for the partner organisation to perform a task in the public interest or for their official functions, and the task or function has a clear basis in law
		* **Legitimate interests** – necessary for the partner organisations legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests (this cannot apply if you are a public authority processing data to perform your official tasks)
	6. The Data Use and Access Act (DUAA) in June 2025 introduced a new, seventh lawful basis under UKGDPR, that of **Recognised Legitimate Interests** - where processing is necessary for disclosure to a person carrying out a public interest task, public security, crime detection, investigation and prevention, protection of a data subject’s vital interests, and safeguarding vulnerable individuals.  As this basis has only just been introduced, agencies should look to their internal or local protocols/agreements when considering use of this basis.
	7. All partner organisations as data controllers are legally obligated to always record and document their lawful bases for processing data, including when sharing for safeguarding reasons per the remit of this Agreement.
	8. Partner organisations where they rely on any of the stated lawful bases stated above (excluding consent) are also legally mandated to inform all data subjects of the data processing of their data.
	9. Emergency and/or life-threatening situations may warrant the sharing of relevant information immediately with the relevant emergency services. This should be covered in partners’ privacy notice information (or specific service information sheet).
	10. All partner organisations must ensure that decisions regarding the sharing of information are clearly recorded regardless of whether consent has been obtained. This includes documenting the rationale behind the decision to share or not share, the legal basis under which it was made, and how it aligns with relevant legislation.
4. **Consent and Mental Capacity**
	1. The presumption is that an adult has capacity to make decisions unless there is reason to think otherwise. Where there is reason to doubt, then a mental capacity assessment needs to be completed and where the outcome is that the person lacks capacity, a best interest’s decision must be made about whether it is appropriate to share information.
	2. An adult may have capacity to make certain decisions on one occasion but not on another, as capacity may fluctuate, or one scenario may be more complex than another. Therefore, if an adult lacks capacity to decide on one occasion, it does not necessarily follow the same decision would be made on another occasion. It should be checked if a new decision should be made.
	3. Please see appendix X which provides some case scenarios around Mental Capacity and consent to share information.
5. **Data Protection/Liaison Officers**
	1. In order to ensure that personal information is exchanged in the most efficient, effective and safe manner, Statutory Organisations will have a designate Responsible Officer. In selecting/appointing such officers Statutory Organisations must identify the minimum number of officers needed in order to retain operational effectiveness, dependent on the size and structure of the organisation.
	2. These Officers should have responsibility for:
		* data protection (subject access)
		* promoting good data quality
		* confidentiality
		* security of holding and the safe transmission of data
		* compliance
		* audit and monitoring
		* complaints procedure (unless a separate internal procedure applies)
	3. Where there is doubt as regards whether there is justification for disclosure of personal information, the safeguarding leads and the Data Protection/Liaison Officer of the relevant organisation should be consulted. In cases of doubt, legal advice should be obtained and in the event the disagreement cannot be resolved, use of sec 45 by the SAB should be considered.
6. **Raising concerns and whistleblowing**
	1. Frontline staff and volunteers should always report safeguarding concerns in line with their organisation’s policy. Internal reporting procedures must not delay information sharing to ensure immediate safety is addressed in emergency situations.
	2. Organisations should have clear routes for escalation of concerns where a member of staff feels a manager has not responded appropriately to a safeguarding issue as well as when there are challenges regarding information-sharing between agencies.
	3. All organisations must have a whistleblowing policy, and all staff should be aware of its contents and when to action it.
	4. The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.
7. **Keeping data safe: exchange storage and retention**
	1. Whilst personal information must be destroyed when it is no longer required for the purpose for which it was provided, it is for the organisation which generated that information (the “data controller”) to make the decision about when the information should be destroyed. What happens to documentation and data may be subject to separate contractual requirements which already exist between the organisations. It is for the organisation supplying information and the organisation receiving it to make sure that each knows how the data is going to be stored and when it will be returned.
	2. The retention and destruction policies of the organisations must be mutually compatible
	3. Any information relating to allegations of sexual abuse must be kept indefinitely in line with the existing requirements of the Independent Inquiry into Child Sexual Abuse (IICSA) requirements. This information must be easy to identify, should it be needed.
8. **Security**
	1. The level of access to personal data is the responsibility of the Responsible Officer within organisations, who is responsible for the security measures outlined above and the maintenance and security of passwords. An effective security policy must be in place in each Statutory Organisation in accordance with the stipulations of the DPA and the UK GDPR.
	2. At minimum, all data assets must be classified and managed in accordance with each agencies protective marking protocols.
	3. Data sent by email must be sent via a secure email system or encrypted/password protected where secure email is not available.
	4. Databases holding personal information must have a defined security and system management procedure for the records and documentation.
	5. The use of all removable media devices is prohibited unless specific authorisation for the use of the device has been obtained from the relevant Organisation’s Responsible Officer. If authorised, Thames Valley Police will only use secure encrypted devices to transfer police information.
9. **Individual Responsibilities**
	1. Every individual working for the partner organisations is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.
	2. Every individual should know how to obtain, use and share information they legitimately need to do their job.
	3. Every individual has an obligation to request proof of identity or takes steps to validate the authorisation of another before disclosing any information requested under this Protocol.
	4. Every individual should uphold the general principles of confidentiality, follow the guidelines set out in this Protocol and seek advice when necessary.
	5. Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.
	6. Every individual should be aware of their duties to report suspected breaches when data may have been shared inappropriately, to their data protection officer, in line with existing arrangements
10. **Information sharing with regards to Safeguarding Adult Reviews**
	1. As part of the statutory function of the Safeguarding Adults Board there is a requirement to conduct Safeguarding Adult Reviews (SAR) when a situation has arisen that meets the criteria for commissioning a SAR under s44 of the Care Act.
	2. All agencies, statutory or otherwise, have a Duty to cooperate with a SAR, including through the gathering and sharing of information as requested by the Safeguarding Adults Board, in order that its statutory function can be discharged.
	3. The sharing of information should include the value of working closely with extended family members. Information should be sought from extended families and carers to inform assessments as a matter of course, unless there are clear reasons why it is not appropriate to do so.
11. Freedom Of Information Requests
	1. The Safeguarding Partnership is not a public body under the Freedom of Information Act (FOIA) and, therefore, is not obliged to respond to any FOI requests, Individual publicly funded Authorities are subject to the Freedom of Information Act and may be required to disclose certain information subject to any exemptions under the FOIA as controller of that data outside of this protocol.

**END**

1. **The Categories are: personal data revealing racial or ethnic origin; personal data revealing political opinions; personal data revealing religious or philosophical beliefs; personal data revealing trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health; data concerning a person’s sex life; and data concerning a person’s sexual orientation.** [↑](#footnote-ref-2)