**Version: May 2018**

**Review: May 2020**

# Oxfordshire Safeguarding Adults Board

# Information Sharing Protocol

## 1. The Purpose of this Protocol

1.1. This protocol forms the basis for the lawful exchange of information between all organisations working with adults with care and support needs (referred to as "the adult") in Oxfordshire:

- Oxfordshire County Council (adult services)
- Thames Valley Police
- Clinical Commissioning group
- NHS England
- Oxford University Hospital
- Oxford Health NHS Foundation Trust
- South Central Ambulance Service
- Oxford City Council
- West Oxfordshire District Council
- South Oxfordshire District Council
- Cherwell District Council
- Vale of White Horse District Council
- National Probation Service
- Thames Valley Community Rehabilitation Company
- "Partner Organisations"

1.2. 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 DPA 2018 and the GDPR.

1.3. 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.

1.4. The protocol applies to all staff employed by the organisations: permanent or temporary, consultants, casual, agency workers and any volunteers.

1.5. It refers to all and any information held on a computer system (in the cloud or hard copy) or on paper including personal data and sensitive personal data as

defined in the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (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 the existing policies in place about how information can be shared and how documents must be marked.

1.6. There are existing legal requirements and protocols in place which cover when information should be shared between the Oxfordshire County Council 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 when police require information immediately, in which case this protocol will apply with regards to providing the information needed to address that emergency.

1.7. 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 date safe: exchange storage and retention

## 2. Confidentiality

2.1. Information (data) which is either “personal” or” sensitive personal “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.

2.2. “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.

2.3. “Sensitive personal data” consists of the following information about an adult: their racial or ethnic origin, political opinion, religious or other similar beliefs, trade union membership, physical or mental health, sex life and the suggestion of committing an offence or a criminal record. This information is afforded particular protection and careful consideration should be given before sharing it.

2.4. 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.

## 3. Reasons for sharing information

3.1. 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.

3.2. 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 a co -ordinated service to those adults receiving services and support from the organisations.

3.3. 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

3.4. Appropriate information sharing is essential to provide a coordinated service to those adults receiving services and support from the organisations. 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 his/her health
- in the public interest to prevent harm to others

3.5. The seven golden rules of information sharing are:

- the DPA, 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)

## 4. Consent and when it is unnecessary or inappropriate to secure it

4.1. The starting point is that the consent of the adult whom the information is about should be secured when appropriate.

4.2. The duty of confidentiality is not absolute and there are occasions when it is appropriate to share information which is otherwise confidential. All 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.

4.3. Adults should be advised about the situations when information will be shared between the organisations and when their consent will be sought or otherwise.

4.4. Consent may be implied in certain situations and this is acceptable.

4.5. 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 “best interests” decision must be made about whether it is appropriate to share information, save where it is an emergency or consent would not normally be sought. An adult may have capacity to make certain decisions about disclosure 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 whether information should be shared, 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.

4.6. There are rare occasions when it is still appropriate to share information even when consent is refused and so overrule the wishes of the adult. If there is time, it is recommended that specialist advice is taken or that it is discussed with a manager prior to sharing. It is a significant step to overrule the wishes of the adult. The reasons for the decision to share must be recorded.

4.7. Emergency and/ or life-threatening situations may warrant the sharing of relevant information immediately with the relevant emergency services. Again, a note should be kept giving reasons as to why the decision to share information was made, in the absence of considering asking for consent.

## 5. Data Protection/Liaison Officers

5.1. In order to ensure that personal information is exchanged in the most efficient, effective and safe manner, Statutory Agencies will designate Data Protection Officers/Data Liaison Officers. In selecting/appointing such officers Statutory Agencies must identify the minimum number of officers needed in order to retain operational effectiveness, dependent on the size and structure of the organisation.

5.2. These Officers should have responsibility for:

- Data protection (subject access)
- Data quality
- Confidentiality
- Security of holding and the safe transmission of data
- Compliance
- Audit and monitoring
- Complaints procedure (unless a separate internal procedure applies)

5.3. There is a list of the contact details of data protection liaison officers attached to this document.

5.4. Where there is doubt as regards whether there is justification for disclosure of personal information, the Data Protection/Liaison Officer of the relevant Agency should be consulted. In cases of doubt, legal advice should be obtained.

## 6. Raising concerns and whistleblowing

6.1. Frontline staff and volunteers should always report safeguarding concerns in line with their organisation's policy – this is usually to their line manager in the first instance except in emergency situations.

6.2. 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.

6.3. All organisations must have a whistleblowing policy and all staff should be aware of its contents and when to action it.

6.4. 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

7.1. 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.

7.2. The retention and destruction policies of the organisations must be mutually compatible

7.3. Any information relating to allegations of sexual abuse must be kept indefinitely in line with the existing requirements of the Goddard Enquiry requirements. This information must be easy to identify, should it be needed.

## 8. Security

8.1. The level of access to personal data is the responsibility of the Data Protection/Liaison Officer 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 Agency in accordance with the stipulations of the DPA 2018 and the GDPR.

8.2. At minimum, all data assets must be classified and managed in accordance with the Government Protective Marking Scheme (GPMS).

8.3. Data sent by email must be sent via a secure email system (e.g. GCSX, PNN, GSX, Gist, CJSM, NH net & N3) or encrypted/password protected where secure email is not available. Thames Valley Police will transfer police information which is GPMS classified as RESTRICTED by secure email.

8.4. Databases holding personal information must have a defined security and system management procedure for the records and documentation.

8.5. The use of all removable media devices is prohibited unless specific authorisation for the use of the device has been obtained from the relevant Agency's Data

Protection/Liaison Officer. If authorised, Thames Valley Police will only use secure encrypted devices to transfer police information.

## 9. Individual Responsibilities

9.1. Every individual working for the Partner Organisations is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

9.2. Every individual should know how to obtain, use and share information they legitimately need to do their job.

9.3. 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.

9.4. Every individual should uphold the general principles of confidentiality, follow the guide-lines set out in this Protocol and seek advice when necessary.

9.5. 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.

9.6. 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