

OXFORDSHIRE SAFEGUARDING CHILDREN BOARD
Information Sharing Protocol

Introduction

This Protocol forms the basis for the lawful exchange of information between all organisations working with children and young people in Oxfordshire.

These organisations are referred to in this Protocol as Statutory Agencies (paragraph 3). All other organisations, including voluntary organisations, who sign up to this Protocol shall be regarded as Statutory Agencies for the purpose of this document¹.

This Protocol covers:

- Obligations under this Protocol
- The principles of lawful data exchange
- Confidentiality & Consent
- Information Governance
- Indemnity
- Summary of legal framework for sharing information

1.1. Sharing information is vital for early intervention to ensure that children and young people with additional needs get the services they require. It is essential to protect children and young people from suffering harm from abuse or neglect and to prevent them from offending. This Protocol is based on the DE Information Sharing Guidance issued as part of Every Child Matters.

1.2. The sharing of information amongst professionals working with children and their families is essential. In many cases it is only when information from a range of sources is put together that a child can be seen to be vulnerable, in need or at risk of harm. Appropriate sharing with other practitioners and agencies is essential if children and families who may be in need of support and services are to be identified at an early stage before problems become serious. Sharing can also enable information from different cases to be put together and assist the process of assessing levels of concern and any potential risks.

1.3. In many instances a failure to pass on information, that might have prevented a child suffering harm, would be far more serious and dangerous than an incident of unjustified disclosure.

1.4. Where there are concerns that a child may be being abused, there is no legal or ethical restriction on sharing information between child protection agencies. In most child protection investigations it would be highly unusual to request consent during the initial phase of an investigation because of the high risk of compromising the investigation. This is particularly the case when Police Officers and Social Workers are conducting a joint investigation. Information should always be exchanged when such disclosure is necessary for the purposes of child protection.

¹ * Note: Section 115 of the Crime and Disorder Act 1998 does not apply to voluntary groups (see para 9.3).

1.5. There is nothing to prevent disclosure of confidential information if certain conditions are met.

In summary, sharing information between agencies is lawful if:

- 1.5.1. Consent is given; or
- 1.5.2. The public interest in safeguarding the child's welfare overrides the need to keep the information confidential; or
- 1.5.3. Disclosure is required under a statutory obligation eg. Local Authority duty to investigate all cases where there is reasonable cause to suspect a child is suffering or is likely to suffer significant harm (Section 47 Children Act 1989).

1.6. A more detailed summary of the law relating to information sharing is set out as a document at **Annex A**.

2. Duty to Co-Operate

2.1. There is an obligation on any local authority, National Health Service Commissioning Board, Clinical Commissioning Group and any Local Housing Authority to co-operate and assist the Local Authority in fulfilment of its statutory obligations (Section 27 Children Act 1989).

2.2. Where there is a duty to co-operate and a clear need to share information there is an obligation on Statutory Agencies to share that information, provided this is for a legitimate purpose.

3. Management of the Protocol

3.1. This Protocol covers the exchange of information/welfare issues between all Statutory Agencies that belong to Oxfordshire Safeguarding Children Board; these Authorities are:

3.1.1. Oxfordshire County Council

- Children, Education & Families Directorate
- Oxfordshire Youth Offending Service
- Chief Executive's Office
- Social and Community Services
- Oxfordshire Drug and Alcohol Action Team (DAAT)
- Public Health Directorate

3.1.2. Thames Valley Police

3.1.3. Thames Valley Probation Service

3.1.4. NHS Commissioning Board

3.1.5. Oxfordshire Clinical Commissioning Group

3.1.6. Oxford University Hospital

3.1.7. Oxford Health NHS Foundation Trust

3.1.8. Oxfordshire Learning Disability Trust

3.1.9. South Central Ambulance Service

3.1.12. Children and Family Court Advisory and Support Service (CAFCASS)

3.1.15. Oxford City Council

- 3.1.16. West Oxfordshire District Council
- 3.1.17. Vale of White Horse District Council
- 3.1.18. South Oxfordshire District Council
- 3.1.19. Cherwell District Council

3.2 These Agencies that have signed up remain bound by the Protocol for all information they held at the date of ceasing to be signatories.

4. Obligations under this Protocol

4.1. It is the responsibility of all signatories to this Protocol to ensure that data exchanges are justified by, and in accordance with:

- 4.1.1. the principles of data protection as enshrined in the Data Protection Act 1998;
- 4.1.2. the justification for the disclosure of confidential information with regard to the rights of a Data Subject under Common Law;
- 4.1.3. The Human Rights Act 1998 and the circumstances in which disclosure is necessary;
- 4.1.4. the statutory responsibilities conferred on the Statutory Agencies by the Children Act 1989, other relevant legislation and the requirements relating to associated guidance; and to
- 4.1.5. ensure that information provided under the terms of this Protocol is not disclosed to any third party without clear reason and justification; and to
- 4.1.6 ensure that all officers/employees handling personal data for the purposes of this protocol must be trained in Information Governance and Data Protection awareness

5. Data Exchange

5.1. General Principles

5.1.1. All data exchanged between Statutory Agencies under this Protocol must be:

- In accordance with the law;
- Relevant to all necessary actions undertaken to protect children;
- Sufficiently detailed for the specified purpose;
- In circumstances justifying the need to share information; and
- Shared in a secure manner;
- Information exchanged must be used only for the purposes for which it was shared.

5.1.3. Signatories to this Protocol must have regard to the DFES 'Seven Golden Rules for Information Sharing' (**Annex B**).

ITEM 05.3

5.1.4. The Police have their own particular rules on information sharing and retention as set out in the Code of Practice in the Management of Police Information. It states that sharing police information must satisfy one of the following policing purposes:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice;
- duty under statute or common law.

Where there is any conflict between this Protocol and MoPI, the Police will regard MoPI as taking precedence.

6.– Legal Gateways for Sharing

6.1. A public authority must have some legal power entitling it to share the information.

6.2. Some concerns regarding children where information will need to be shared under this agreement will often fall below a statutory threshold of Section 47 or even Section 17 Children Act 1989. If they do however fall within these sections of the 1989 Act then these sections will be the main legal gateway.

6.3 Sections 10 and 11 of the Children Act 2004 place obligations upon Local authorities, police, clinical commission groups and the NHS Commissioning Board to co-operate with other relevant partners in promoting the welfare of children and also ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

6.4 Section 10 and 11 of the Children Act 2004 create a 'permissive gateway' for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information namely the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law duty of confidentiality.

6.5 Section 29 of the Data Protection Act 1998 does not give a direct power to disclose information, it does however state 'that if not disclosing information would prejudice the prevention/detection of crime and/or the apprehension/ prosecution of offenders, personal data can be disclosed'.

6.6 If by not disclosing information to the relevant signatories of this Protocol would prejudice the situations listed above, signatories are exempt from the usual non-disclosure provisions and may provide the information requested / they wish to share proactively.

6.7 All decisions to share or not share information **must** be decided on a case-by-case basis and recorded.

7. The Duty of Confidence and Obtaining Consent

ITEM 05.3

7.1 The starting point in relation to sharing information is that practitioners will be open and honest with families and individuals from the outset about why, what, how and with whom information will or could be shared.

7.2 It may be necessary and desirable to deviate from the normal approach of seeking consent from a family in cases where practitioners have reasonable grounds for believing that asking for consent would be unsafe or inappropriate. For example if there is an emergency situation or if seeking consent could create or increase a risk of harm.

7.3 There must be a proportionate reason for not seeking consent and the person making this decision must try to weigh up the important legal duty to seek consent and the damage that might be caused by the proposed information sharing on the one hand and balance that against whether any, and if so what type and amount of harm might be caused (or not prevented) by seeking consent.

7.4 There is no absolute requirement for signatories to obtain consent before sharing information nor there a blanket policy of never doing so. There is an obligation to consider on all occasions and on a case by case basis whether information will be shared with or without consent. This determination by a practitioner should always be reasonable, necessary and proportionate. It should always be recorded together with the rationale for the decision.

7.5 Parents should be informed of any referral and their permission sought to share information with other agencies unless to do so would:

- be prejudicial to the child's welfare
- cause concern about the behaviour of the adult concerned with the child
- cause concern that the child would be at risk of further significant harm

7.6 Any decision not to see parental consent needs to be recorded with reasons.

7.7. When considering whether the principles of confidentiality are overridden, the following should be considered:

7.7.1. It may be inappropriate or impossible to obtain the consent of an alleged perpetrator, if consent is likely to be withheld. The Data Protection Act allows disclosure of information for the prevention / detection of crime, or the apprehension/prosecution of offenders. Assessment must be made on a case-by-case basis.

7.7.2. With regard to third parties their consent to disclosure should be obtained if possible and reasonable in all the circumstances.

7.7.3. It is in the public interest to maintain a high standard of confidentiality so that people will have the confidence to come forward with their complaints or information.

7.7.4. Implied consent may often be present when there is a reasonable expectation on the person providing the information that all necessary and appropriate action would be taken.

ITEM 05.3

7.8. Children are entitled to the same duty of confidentiality as adults provided that they have the ability to understand the choices and consequences. If, however, it is considered that a child is under the undue influence of another person (eg. In perhaps a case of alleged sexual abuse), confidentiality to the child may need to be overridden in order to safeguard the child.

7.9. There are specific ethical difficulties in balancing the interests or confidentiality of the children and parents or carers' right to know the issues of concern. A balance needs to be struck between competing obligations and specialist advice in those circumstances should always be sought.

7.10. If the disclosure of personal information is necessary or expedient, the power to disclose must be present either:

7.10.1. in the public interest to prevent harm to others;

7.10.2. under the statutory obligations to investigate the risk to children set out in the Children Act 1989;

7.10.3. is in the interests of the Data Subject eg. In relation to his/her health;

7.10.4. if appropriate, with the consent of the Data Subject.

7.11. Where personal data is required for child protection purposes even when consent has not been sought or given, the rules applicable to confidentiality still applies. Assessments should be made on a case by case basis whether:

7.11.1. the disclosure is necessary to support child protection action;

7.11.2. the public interest is of sufficient weight to override the presumption of confidentiality; and

7.11.3. the information is being processed fairly.

INFORMATION GOVERNANCE

8. Data Protection/Liaison Officers

8.1. 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.

8.2. These Officers should have responsibility for:

8.2.1. Data protection (subject access);

8.2.2. Data quality;

8.2.3. Confidentiality;

8.2.4. Security of holding and the safe transmission of data;

8.2.5. Compliance;

8.2.6. Audit and monitoring;

ITEM 05.3

8.2.7. Complaints procedure (unless separate procedure applies).

8.3. 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 continued doubt or uncertainty, legal advice should be obtained.

8.4. With regard to complaints, any investigation will examine the process that led to the provision of data and will be handled by the Data Protection/Liaison Officer (unless a separate procedure applies). Ideally, this Officer will be the first point of contact for any complaints. This arrangement does not remove the right for complaints to be made directly to the Information Commissioner (formally the Data Protection Registrar).

8.5 Each Agency should provide the names of all current Data Protection/Liaison Officers within their agency to the OSCB Business Manager who will retain a central register.

9. Security

9.1. 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 Data Protection Act 1998.

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

9.3. Data sent by email must be sent via a secure email system (e.g GCSX, PNN, GSX, GSi, CJSM, NHSnet & 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.

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

9.5. 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.

10. Secondary Use of Data

10.1. No secondary i.e. no further disclosure is permitted under this Protocol unless in full compliance with an agency's statutory obligations or in accordance with OSCB procedures. Any requests for information by or for external organisations or other third parties should normally be made to the Data Holding Agency.

11. Data Quality

ITEM 05.3

11.1. Information shared between Statutory Agencies should be either factual or constitute relevant personal data.

11.2. Personal data found to be inaccurate should be notified to the authority owning the data. That authority will be responsible for:

11.2.1. Correcting the information;

11.2.2. Notifying all other recipients of this data (who, upon being notified of inaccuracy, are responsible for relevant data in their possession being corrected).

11.3. Data retained by Statutory Agencies should be regularly monitored, the frequency of such monitoring dependent on the type of data. Any corrections or amendments made to shared information must be made known to the Statutory Agencies which also retain that particular information within fourteen days.

12. Retention and/or Destruction

12.1. Personal information must be destroyed when it is no longer required for the purpose for which it was provided;

12.2. All Statutory Agencies should retain information relating to child protection as long as it is necessary for not only the protection of the child but possibly other children and a specified retention period should take into account the importance of retaining this information for future investigations (NOTE: Care Proceedings and Adoption papers are retained for a period of 75 years);

13. Documentation

13.1. Requests for information to be shared between Relevant Authorities should be made in writing unless the matter is urgent in which case the request or reply should be followed up in writing.

13.2. A written response from a Data Holding Agency should be made within fifteen working days to such a request for information.

13.3. Any subsequent disclosure of information should record:

13.3.1. The source of the data;

13.3.2. The Data Holding Agency as originator of the data. This must be specific as the exchange of data may continue for several years, new staff will be involved and the original agreement may get watered down;

13.3.3. What data was originally requested. In certain circumstances this may differ from what was actually permitted to be disclosed;

13.3.4. Grounds/justification for disclosure (including why public interest outweighs the duty of confidentiality);

ITEM 05.3

13.3.5. What data has been disclosed with particular reference to the degree of personal data shared;

13.3.6. Who and which organisations have received the data;

13.3.7. What time-limits apply to the sharing of data;

13.3.8. Details of any extensions to these time-limits;

13.3.9. Whether (subsequently) there has been any secondary disclosure of the data; and

13.3.10. Amendments to the quality of the data.

13.4. Forms used for the exchange of data must be signed and dated with copies retained by all parties to the disclosure.

13.5. Decisions made on the basis of disclosed personal data should be minuted.

14. Indemnity

13.1. Each agency (“indemnifying agency”) will indemnify and keep indemnified all other agencies who are part of this Protocol form and against any and all loss, damage or liability (whether criminal or civil) suffered and legal fees and costs incurred by the other agencies resulting from any negligent act or omission and/or a breach of this protocol by the indemnifying agency including:

14.1.1. Any act negligent or default of the indemnifying agencies, employees or agents; or

14.1.2. Breaches resulting in any successful claim by any third party arising out of the wrongful disclosure of any information by the indemnifying agency.

15. Data Subject Access

15.1. The Data Subject’s right to access his/her personal data is not affected by this Protocol. An application by the Data Subject should be made to the Statutory Agency that is in possession of the data. In accordance with the Data Protection Act 1998 all forms and information exchanged under this Protocol will be considered to be third party information if such an application is made i.e. if holding information received from another agency, then that agency’s consent should normally be sought.

ANNEX A

Information Sharing Briefing Summary of the Legal Position

1. Introduction

1.1 The main legal framework relating to the protection of personal information is set out in:

1.1.1 The Human Rights Act 1998, which incorporates Article 8 of the European Convention on Human Rights (ECHR), including the right to a private and family life;

1.1.2 The common law duty of confidentiality; and

1.1.3 The Data Protection Act 1998.

1.2 Some Acts of Parliament give public bodies express statutory powers to share information.

1.3 Where there is no express statutory power to share information it may still be possible to imply such a power from the other duties and powers public bodies have.

2. Human Rights Act 1998

2.1. All statutory agencies have a pro-active responsibility to ensure that no person should be subjected to inhuman or degrading treatment in accordance with Article 3 of the European Convention on Human Rights.

2.2. In addition, the right to a private and family life described in Article 8 is subject to lawful interference by a public authority only where it is necessary to:

2.2.1. prevent disorder or crime

2.2.2. protection of health or morals

2.2.3. protection of rights and freedom of others

2.3. Clearly, if disclosure falls within these exemptions then it is entirely appropriate, necessary and in accordance with the Human Rights Act 1998. The proportionality test as specified in the common law duty of confidence similarly applies. There remains a degree of justification on disclosure decisions but the Human Rights Act does not prevent sharing of information and indeed in child protection cases requires sharing of information in order to fulfil these statutory responsibilities.

3. The Common Law Duty of Confidentiality

3.1. The common law provides that where there is a confidential relationship, the person receiving the confidential information is under a duty not to pass on the information to a third party. However, this duty is not absolute and information can be shared without breaching the common law duty if:

ITEM 05.3

- 3.1.1. the information is not confidential in nature; or
- 3.1.2. the person to whom the duty is owed has given explicit consent; or
- 3.1.3. there is an overriding public interest in disclosure; or
- 3.1.4. sharing is required by a court order or other legal obligation.

3.2. Is the Information Confidential?

3.2.1. Some information is clearly confidential and special arrangements need to be made to safeguard from unjustified or accidental disclosure. The confidentiality that attaches to this is not absolute in all circumstances and where there is a clear need to disclose then provided the correct procedure is followed and there is clear justification this can be done. Some information may not be confidential, particularly if it is trivial or readily available from other sources or if the person to whom it relates would not have an interest in keeping it secret. For example, a Social Worker who was concerned about a child's whereabouts might telephone the School to establish whether the child was in School that day.

3.2.2. The Courts have found a duty of confidentiality to exist only when:

- A contract provides for information to be kept confidential, or
- There is a special relationship between parties, such as patient and Doctor, Solicitor and client, teacher and pupil, or
- An agency or a Government Department, such as Inland Revenue, collects and holds personal information for the specific purposes of its functions.

3.3. Maintaining Confidentiality

3.3.1. As a general rule you should treat all personal information you acquire or hold in the course of working with children and families as confidential and take particular care that sensitive information is held securely.

3.4. Disclosure by Consent

3.4.1. There will be no breach of confidence if the person to whom a duty of confidence is owed consents to the disclosure. Consent can be express (that is orally or in writing) or can be inferred from the circumstances in which the information was given (implied consent). Implied consent is appropriate for the sharing of 'personal' information however consent may be required for the sharing of 'sensitive personal' data (see section 7 for further details).

3.5. Whose Consent Is Required?

3.5.1. The duty of confidence is owed to the person who has provided information on the understanding it is to be kept confidential and, in the case of medical or other records, the person to whom the information relates.

3.6. Has Consent Been Given?

3.6.1. When sharing personal information you do not need express consent if you have reasonable grounds to believe that the person to whom the duty is

ITEM 05.3

owed understands and accepts that the information will be disclosed. For example, a person who refers an allegation of abuse to a Social Worker would reasonably expect that information to be shared on a “need to know” basis with those responsible for investigating and following up the allegation. Anyone who receives information, knowing it is confidential, is also subject to the duty of confidence. Whenever you give or receive information in confidence you should ensure that there is a clear understanding as to how it may be used or shared.

3.6.2. Professionals should avoid giving absolute guarantees as to confidentiality, particularly when dealing with disclosures from children. In such cases it should be made clear from the outset that what is said will be treated in confidence but such information may need to be passed on to other professionals who may need to know.

3.7. Should I Seek Consent?

3.7.1. If consent is given then it is absolutely clear to all concerned that there is no problem whatsoever in sharing information. Whilst consent will provide a basis on which organisations can share personal data, this is not always achievable or desirable. For example, you should not ask for consent in circumstances where you think this will be contrary to the child’s welfare. For example, if the information is needed urgently then the delay in obtaining consent may not be justified. Seeking consent may prejudice a Police investigation or may increase the risk of harm to the child.

3.8. What If Consent Is Refused?

3.8.1. It is bad practice to offer individuals a ‘choice’ if the data sharing is going to take place regardless of their wishes, for example where it is required by statute or is necessary for the provision of an essential service.

3.9. Capacity

3.9.1. Where the Data Subject does not have capacity to give consent to share, consent may be sought from someone who may appropriately act on behalf of the Data Subject, for example an appropriate adult or someone who holds a relevant Power of Attorney.

4. Disclosure in the Absence of Consent

4.1. The law recognises that disclosure of confidential information without consent or Court Order may be justified in the public interest to prevent harm to others.

4.2. There will be some circumstances where you should not seek consent from the individual or their family, for example: where to do so would place a person at increased risk of significant harm; or it would prejudice the prevention, detection or prosecution of a serious crime; or lead to unjustified delay in making enquiries about allegations of significant harm to a child.

4.3. The key factor in deciding whether or not to breach confidentiality is proportionality: i.e. is the proposed disclosure a proportionate response to the need

ITEM 05.3

to protect the welfare of the child. The amount of confidential information disclosed, and the number of people to whom it is disclosed, should be no more than is strictly necessary to meet the public interest in protecting the health and wellbeing of a child. The more sensitive the information, the greater the child centred need must be to justify disclosure and the greater the need to ensure that only those professionals who have to be informed receive the material (“the need to know basis”).

4.4. The “Need to Know” Basis

Relevant factors:

- 4.4.1. What is the purpose of the disclosure?
- 4.4.2. What is the nature and extent of the information to be disclosed?
- 4.4.3. To whom is the disclosure to be made (and is the recipient under a duty to treat the material as confidential)?
- 4.4.4. Is the proposed disclosure a proportionate response to the need to protect the welfare of a child to whom the confidential information relates.

4.5. It is, therefore, essential that there is a clear record of the reasons and justification for disclosure so as to demonstrate that the decision is reasonable, proportionate and fully justifiable.

5. The Duty of Confidentiality to Children and Young People

5.1. Children are entitled to the same duty of confidentiality as adults provided that they have the ability to understand the choices and consequences. If, however, it is considered that a child is under the undue influence of another person (eg. In perhaps a case of alleged sexual abuse) confidentiality to the child may need to be overridden in order to safeguard the child.

6. Data Protection Act 1998

6.1. The Data Protection Act 1998 (“the Act”) regulates the handling of personal data. ‘Personal’ data is that which can identify a living individual. Some personal data is classified as ‘sensitive personal’ when it relates to a person’s: racial or ethnic origins, physical or mental health, sexual life, criminal offences, religious beliefs and trade union membership. The Act lays down requirements for the processing of this information, which includes obtaining, recording, storing and disclosing it. Organisations, which process personal data must comply with the 8 Data Protection principles.

6.2. Where there is a legitimate reason for sharing “personal” information and one of the conditions in Schedule 2 of the Act apply then the information can be disclosed. Examples of Schedule 2 conditions are:

- 6.2.1. the Data Subject (the person to whom the data relates) consents; or
- 6.2.2. the disclosure is necessary for compliance with a legal/statutory obligation; or
- 6.2.3. it is necessary to protect the vital interests of the Data Subject; or
- 6.2.4. it is necessary for the exercise of a statutory function or other public function exercised in a public interest (eg. Under the Children Act for the purposes of a Section 17 assessment or a Section 47 enquiry); and

ITEM 05.3

6.2.5. it is necessary for the purposes of legitimate interests pursued by the person sharing the information, except where it is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.

6.3. As can be seen there is a condition to cover most situations where a practitioner needs to share information to safeguard a child's welfare. In particular, the last condition (legitimate interest) is relevant in all cases and involves a proportionality test similar to that applied to breaches of confidence.

7. Sensitive Personal Data

7.1. There are additional safeguards within the Act for sensitive personal data relating to the Data Subject's racial or ethnic origins, physical or mental health or conditions, sexual life, criminal offences, clinical opinions, religious beliefs, membership of Trade Union.

7.2. This sensitive personal data can be shared if at least one of the conditions in Schedule 2 AND Schedule 3 of the Act are met. Examples of Schedule 3 conditions are:

- 7.2.1. the Data Subject has explicitly consented to the disclosure;
- 7.2.2. it is necessary to protect the vital interests of the Data Subject or another person where the Data Subject's consent cannot be given or is unreasonably withheld or cannot reasonably be expected to be obtained;
- 7.2.3. it is necessary to establish, exercise or defend legal rights; or
- 7.2.4. it is necessary for the exercise of any statutory functions.

8. Other exemptions

8.1. Personal data are exempt from non-disclosure provisions where the disclosure is for the prevention or detection of crime; the apprehension or prosecution of offenders (Section 29 of the Act).

8.2. Where personal data relates to child protection, the risk of child abuse falls clearly within prevention or detection of an unlawful act.

8.3. The justified and necessary sharing of information between professionals is an essential prerequisite in safeguarding a child's welfare. The Data Protection Act does not prevent sharing of information amongst Children, Education & Families and other agencies in connection with a Section 17 assessment or a Section 47 enquiry.

8.4. If in doubt, if you need advice on Data Protection requirements you should contact your Data Controller who will be able to provide you with advice on the Data Protection requirements.

9. Express of Implied Powers to Share Information

9.1. The Children Act 1989

ITEM 05.3

9.1.1. There is an obligation on Local Authorities, Health Service, Clinical Commissioning Group, Hospital Trusts and any Local Housing Authority to co-operate and assist the Local Authority in fulfilment of its statutory obligations (Section 27 Children Act 1989).

9.1.2. Section 47 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm.

9.1.3. Under Section 17 of the Children Act 1989 the Local Authority have a statutory duty to safeguard and promote the welfare of children within their area who are in need. Again, in general the law will not prevent you from sharing information with other practitioners if:

9.1.4. those likely to be affected consent, or

9.1.5. the public interest in safeguarding the child's welfare overrides the need to keep the information confidential; or

9.1.6. disclosure is required under a Court Order or other legal/statutory obligation

9.2. The Children Act 2004

9.2.1. The Children Act 2004 Section 10 places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:

- Physical and mental health, and emotional well-being;
- Protection from harm and neglect;
- Education, training and recreation;
- Making a positive contribution to society;
- Social and economic well-being.

9.2.2. The relevant partners must co-operate with the Local Authority to make arrangements to improve children's well-being and are formal members of the Oxfordshire Safeguarding Children Board.

9.2.3. The statutory guidance on this Act states that good information sharing is key to successful collaborative working and that arrangements under Section 10 of the Children Act 2004 should ensure that information is shared for strategic planning purposes and to support effective service delivery. It also states that these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations.

9.2.4. Section 11 of the Act places a duty on key people and bodies to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children. The key people and bodies are:

9.2.4.1. Local Authorities (including District Councils)

- 9.2.4.2. The Police
- 9.2.4.3. The Probation Service
- 9.2.4.4. Bodies within and aligned with the National Health Service
- 9.2.4.5. Oxfordshire Clinical Commissioning Group
- 9.2.4.6. Youth Offending Service
- 9.2.4.7. Governors/Directors of Prisons and Young Offenders Institutes
- 9.2.4.8. Directors of Secure Training Centres
- 9.2.4.9. The British Transport Police

9.2.5. In order to safeguard and promote the welfare of children, arrangements should ensure that:

9.2.6. All staff in contact with children understand what to do and the most effective ways of sharing information if they believe a child or family may require targeted or specialist services in order to achieve their optimal outcome;

9.2.7. All staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including those children suffering or at risk of significant harm.

9.3. Crime and Disorder Act 1998

9.3.1. Section 115 enables any person to disclose information to a relevant Authority for any purposes of the Act if they do not otherwise have the power to do so. Relevant authorities include Local Authorities, NHS Bodies and Police Authorities. The purpose of the Act broadly covers the prevention and reduction of crime in the identification or apprehension of offenders. This act does not provide a power for statutory authorities to disclose information with non-statutory organisations (such as many voluntary organisations) for the same purpose.

10. Other Specific Legislation Containing Express Powers or Which Imply Powers to Share Information

- 10.1. Section 155 and 175 Education Act 2002
- 10.2. Section 13 and Section 434(4) Education Act 1996
- 10.3. Section 117 and 119 Learning and Skills Act 2000
- 10.4. Regulation 6 and 18 Education (SEN) Regulations 2001
- 10.5. Children (Leaving Care) 2000
- 10.6. Protection of Children Act 1999
- 10.7. Section 20 Immigration and Asylum Act 1999
- 10.8. Part 1 Local Government Act 2000
- 10.9. Section 325 Criminal Justice Act 2003

10.10. Section 2 of the National Health Service Act 1977

10.11. The Adoption and Children Act 2002

11. Case Law Decisions

11.1. There have now been a number of decisions dealing with the criteria by which disclosures may be justified and the factors that need to be considered.

11.2. Before a decision is made about disclosure, a professional must consider the following factors, "is there a pressing need to disclose?" i.e.

11.2.1. belief in the truth of the allegation;

11.2.2. legitimacy of the interests of the person needing this information;

11.2.3. degree of risk if disclosure is not made.

11.3. In addition, the following factors may also be important:

11.3.1. the relevance and importance of the information

11.3.2. the urgency of disclosure

11.3.3. whether consent for disclosure has been sought

11.3.4. the interests of the child

11.3.5. the impact upon the person to whom the information relates

11.4. These factors are particularly relevant when details about the Schedule 1 offence might be disclosed if, in the individual circumstances of such cases, the agency feel there is a clear basis for concern that the child may be at risk, and it is entirely appropriate to inform parents or carers of:

11.4.1. The offenders previous convictions;

11.4.2. That this gives rise to a legitimate concern and view of the potential for future abuse (There is well documented research establishing the high rate of reoffending of Schedule 1 offenders. Disclosure may be justified see R v (1) A Police Authority in the Midlands (2) A County Council in the Midlands, ex parte LM1999)

11.5. It is permissible for findings in care proceedings that a child's father constituted a considerable risk to children to be disclosed to the father's Housing Association landlord where there was "real and cogent evidence of a pressing need" for such disclosure (re C (Sexual Abuse: Disclosure 2002))

11.6. Local Authorities have the power to communicate the conclusions of enquiries made under Section 47 of the Children Act 1989 where on the facts of the case it is reasonably believed it was necessary to do so to protect children from the risk of sexual abuse (R v Hertfordshire County Council, ex parte A 2001)

11.7. Each case should be judged on its own facts and disclosure should only be made where there is a pressing need for that disclosure to be made and if possible with the Data Subject being provided with an opportunity to respond to the proposed

ITEM 05.3

disclosure prior to a final decision being taken . This may not be possible within the reasonable time constraints of the investigation. Disclosure must be judged against Article 8 (right to respect for private and family life) and proven to be necessary in all the circumstances. The honest judgement of professional police officers went a long way towards establishing reasonableness (R v Chief Constable of North Wales Police ex parte Thorpe 1998).

11.8. In deciding whether or not to release information relating to a charge of indecency where this was subsequently withdrawn, it was essential that a view be taken that the information was relevant and reliable and proper weight was given to the identification of the claimant and the effect of disclosure on a person's employability. The emphasis was on the need for a proper procedure to ensure that all relevant factors were considered and that the person had a right to make representations before disclosure (R v Chief Constable West Midlands Police (Times Law Report 2nd Feb 2004).

12. Conclusion

12.1. There are no legal barriers whatsoever that prevent the appropriate and necessary sharing of information between agencies in fulfilment of their statutory duties to safeguard and promote the welfare of children, provided that proper agreed procedures are followed.

P G Clark
County Solicitor
May 2014

ANNEX B

Seven Golden Rules for Information Sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.
2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.
4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

ANNEX C – Kingfisher Team

This annex provides specific information about the information sharing carried out between the Kingfisher Team and its partners. It should be read in conjunction with the Oxfordshire Safeguarding Children Board Information Sharing Protocol and any information sharing should be executed in accordance with the requirements set out in it.

Kingfisher Team:

The Kingfisher Team enables partnership working between Police, Child Social Care and Health in a co-located environment. It safeguards and supports children and young people who are being, or are at risk of child exploitation and seeks to identify those who are offending or are likely to offend. This activity supports the above partner's statutory obligations to safeguard children and young people.

This work also satisfies the following wider objectives and policing purposes:

- Protecting life & property

ITEM 05.3

- Preserving order
- Preventing the commission of offences
- Bring offenders to justice
- Duty under statute of common law

Partnership Working:

The Kingfisher Team will work with wider statutory partners and voluntary agencies in order to achieve its safeguarding aims. The following partners / organisations will be working regularly with the Kingfisher Team:

- Social Care – Early Interventions Service
- Heads of state run schools
- Youth Offending Service

Other organisations and charities will be engaged or invited to forums on a case by case basis where they are able to contribute to safeguarding activities:

Information Sharing:

To facilitate effective safeguarding activity, partners will need to share information about relevant offending, offenders and victims. Any information sharing will be carried out in accordance with the requirements documented in the Oxfordshire Safeguarding Children Board Information Sharing Protocol. The following information does not intend to repeat that which is included in the aforementioned protocol but provides additional detail specific to information sharing within the Kingfisher Teams and subsequent safeguarding activity.

Types of information shared:

The Kingfisher Team seeks to draw information together from partners to initially identify those at risk of being a victim or perpetrator of child sexual exploitation and then develop a more detailed picture of risk and required safeguarding activity. This will involve the sharing of relevant information about offenders, victims and their families, where it is necessary, relevant and proportionate to the team's safeguarding aims and the prevention and detection of crime.

More specifically this may include but is not restricted to:

- Personal and sensitive personal information (as defined by the Data Protection Act 1998)
- Relevant previous convictions
- Relevant information about current investigations (where there is no risk of sub judice)
- Relevant intelligence
- School attendance records and any issues at school

Legality of information sharing:

The following statutes represent the more common legal pathways under which information will be shared:

1. Crime & Disorder Act 1998 s.115 – allows sharing for the purposes of reducing crime, disorder and antisocial behaviour; between statutory agencies and organisations who are acting in an official capacity on behalf of them.

ITEM 05.3

However, this will not be a suitable gateway for sharing with non-statutory partners (including many voluntary organisations).

2. Data Protection Act 1998:
 - Informed consent given by the data subject (must be explicit consent when sharing sensitive personal information); OR
 - S.29: for the purposes of preventing / detecting crime or to apprehend / prosecute offenders; OR
 - S.35: required by law in connection with legal proceedings
3. Common law disclosure – where the public interest in disclosing information outweighs the data subject's duty of confidentiality.
4. Children Act 1989: - section 17, 27 and 47.
5. Children Act 2004: - section 10 and 11

Specific information sharing procedures:

Information sharing will be commonplace between the statutory partner members of the co-located Kingfisher Team.

The Kingfisher Team will also chair regular meetings with a wide range of statutory partner agencies and voluntary organisations to gather the information needed to identify persons requiring safeguarding intervention and prevent / detect crime. Where individual cases are discussed in detail the membership will be restricted to those who will contribute towards the safeguarding process; in particular if they are not statutory agencies.

The transfer of shared information must be carried out securely. Thames Valley Police require the use of encrypted email or encrypted portable devices to electronically transfer police information classified under GPMS, up to and including RESTRICTED.

SIGNATORIES TO OSCB INFORMATION SHARING PROTOCOL

Board member organisation	Date
Childrens Social Care, Oxfordshire County Council	13.11.14
Education and Early Intervention, Oxfordshire County Council	12.11.14
Youth Offending Service, Oxfordshire County Council	12.11.14
Oxfordshire Fire and Rescue Service, Oxfordshire County Council	25.11.14
Adult Social Care, Oxfordshire County Council	20.11.14
Oxford City Council	20.11.14
Cherwell District Council	12.11.14
West Oxfordshire District Council	13.11.14
The Warriner School	12.11.11
Windmill Primary School	20.11.14
Abingdon and Witney College	13.11.14
Thames Valley Police	13.11.14
National Probation Service	19.11.14
Oxford University Hospitals	16.11.14
Oxford Health NHS FT	17.11.14
Oxfordshire Clinical Commissioning Service	20.11.14
Oxfordshire Domestic Abuse Service Strategy Group	20.11.14