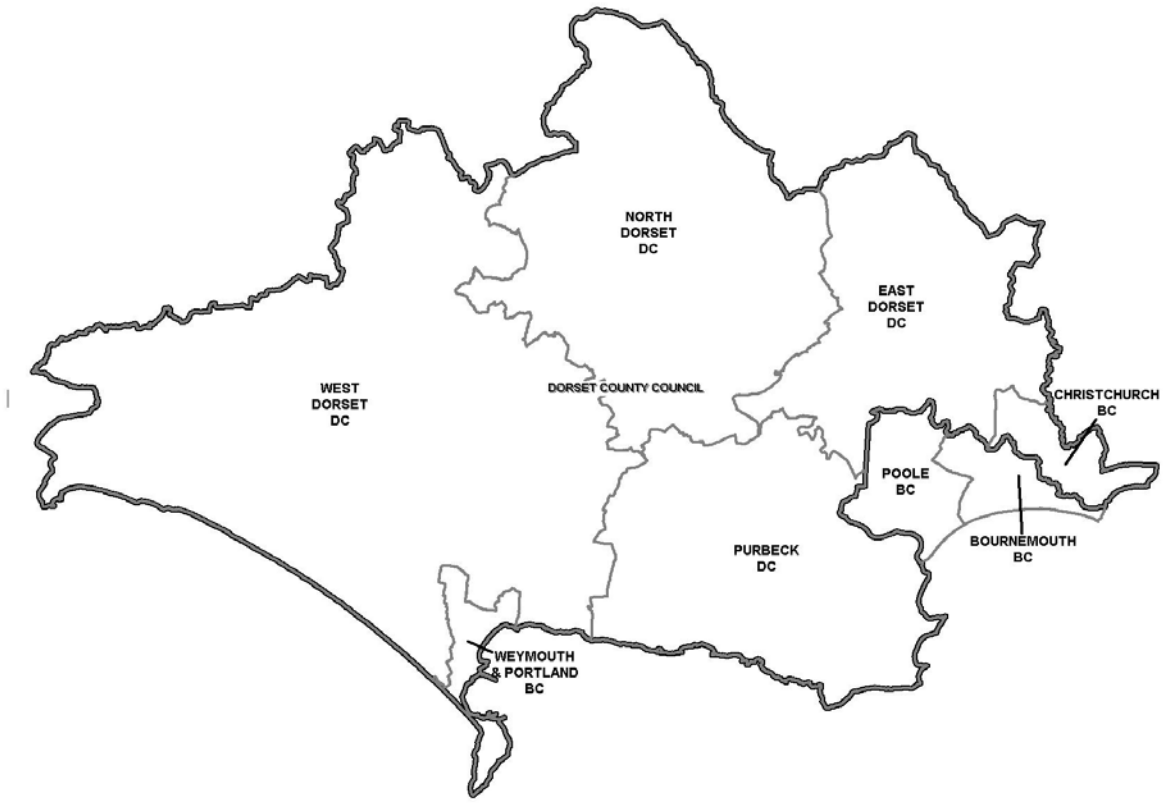
Dorset Overarching Information Sharing Protocol (OAISP)



Version: 1:18 - May 2014

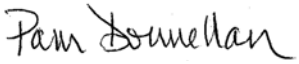
CONTENTS

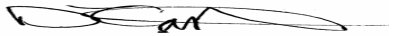
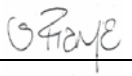
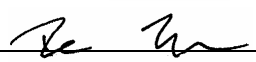
DOCUMENT HISTORY SHEET

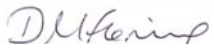
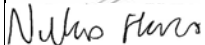
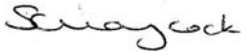
DATE	VERSION	REVIEW / REVISION/ AMENDMANT	DETAILS
01/04/08	V1.0		Document Issue.
01/09/08	V1.1	Amendment	Updated Signatories, Corrected Formatting & Inserted Copyright Notice.
12/01/09	V1.2	Amendment	Additional Signatories Added
13/03/09	V1.3	Amendment	Additional Signatory Added
19/03/09	V1.4	Amendment	Additional Signatory Added
6/10/09	V1.5	Amendment	Additional Signatory Added
21/03/11	V1.6	Amendment	Additional Signatory Added
11/10/11	V1.7	Amendment	Additional Signatory Added
10/05/12	V1.8	Amendment	Additional Signatory Added
18/10/12	V1.9	Amendment	Additional Signatory Added
10/01/13	V1.10	Amendment	Additional Signatory Added
30/01/13	V1.11	Amendment	Additional Signatories Added
21/03/13	V1.12	Amendment	Additional Signatories Added
30/04/13	V1.13	Amendment	Additional Signatories Added
17/09/13	V1.14	Amendment	Additional Signatories Added

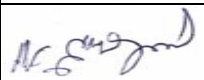
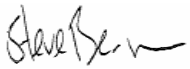
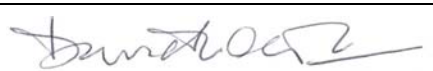
DATE	VERSION	REVIEW / REVISION/ AMENDMANT	DETAILS
31/03/14	**V1.15**	**Amendment**	**Additional Signatories Added**
28/05/14	**V1.16**	**Amendment**	**Additional Signatories Added**

SIGNATORIES TO THE DORSET OVER ARCHING INFORMATION SHARING PROTOCOL (OAISP)

ORGANISATION	POST	NAME	SIGNATURE	DATE
Ability Housing Association	Housing Services Officer	John Williams		4 September 2013
Ansbury	Chief Executive	Martyn Jewell		2 October 2012
Big Issue Foundation (Dorset & Hants)	Dorset & Hampshire Area Service Broker	Simon Chilcott		14 March 2014
Bournemouth Borough Council	Chief Executive	Pam Donnellan		8 May 2008
Bournemouth Churches Housing Association	Company Secretary	Phillip Baker		23 January 2013
Chesil Education Partnership	Chesil Development Leader	Caroline Peer		10 January 2013
Christchurch Borough Council	Chief Executive	Michael Turvey		10 April 2008
Crime Reduction Initiative (CRI)	Service Manager	Rachel Ulyett		12 April 2013
Dorset County Council	Chief Executive	David Jenkins		8 May 2008
Dorset County Hospital NHS Foundation Trust	Chief Executive	Jan Bergman		June 2009

ORGANISATION	POST	NAME	SIGNATURE	DATE
Dorset Fire & Rescue Service	Chief Fire Officer	Darran Gunter		8 May 2008
Dorset HealthCare University NHS Foundation Trust (DHFT)	Chief Executive	Roger Browning		10 October 2011
Dorset Police	Chief Constable	Martin Baker		8 May 2008
Dorset Probation Service	Chief Officer	John Wiseman		8 May 2008
Dorset Rape Crisis Support Centre	Service Manager	Sharon Frame		16 January 2013
Dorset Youth Association	Director	Dave Thompson		21 March 2013
Druglink	Finance Manager	Janice Beaty		15 April 2013
East Dorset District Council	Chief Executive	Alan Breakwell		10 April 2008
East Dorset Housing Association	Managing Director	Nick Fry		4 August 2008
EDP Drug & Alcohol Services	Dorset Team Leader	Sarah Maner		6 March 2014
Essential Drug & Alcohol Services (EDAS)	Chief Executive	Mindi Crespi		23 April 2012
Magna Housing Association	Director	David Aldwinckle		21 June 2008

ORGANISATION	POST	NAME	SIGNATURE	DATE
NHS Bournemouth & Poole	Chief Executive	Debbie Fleming		9 March 2009
NHS Dorset (Dorset Primary Care Trust)	Director of Communications & Corporate Affairs	Claire Warner		7 November 2008
North Dorset District Council	Chief Executive	Liz Goodall		10 April 2008
PAS Supported Housing	Operations Manager	Jo Booth		27 March 2014
Poole Borough Council	Chief Executive	John Mc Bride		8 May 2008
Poole Hospital NHS Foundation Trust	Chief Executive	Sue Sutherland		16 June 2008
Poole Housing Partnership Ltd	Chief Executive	Joe Logan		6 October 2009
Purbeck District Council	Chief Executive	Steve Mackenzie		10 April 2008
Purbeck Housing Trust	Managing Director	Robin James		4 August 2008
Raglan Housing Association	CEO	Nicholas Harris		30 April 2013
Relate Bournemouth, Poole & Christchurch	Centre Manager	Angela Craven		5 December 2013
Relate Dorset & South Wilts	Centre Manager	Sheila Maycock		18 October 2012

ORGANISATION	POST	NAME	SIGNATURE	DATE
Routes to Roots (Poole)	Trustee	Gabriele Sanger-Stevens		17 March 2014
Safe Partnership Ltd	Chief Executive	Dr Malcolm Macleod OBE		26 February 2013
Streetwise Partnership Trust Ltd	Chair of Trustees	Mike Emsley		19 March 2009
Synergy Housing Group	Group Chief Executive	Graeme Stanley		4 August 2008
The Royal Bournemouth & Christchurch Hospitals NHS Foundation Trust	Chief Executive	Tony Spotswood		December 2008
The Steven James Practice	Chair of Board of Governors	Guy Rouquette		10 May 2012
The You Trust	Director of Operations	Sally Hutfield		15 Feb 2013
TIS Counselling	Counsellor	Tom Smith		18 April 2012
Two Saints Limited	Chief Executive	Steve Benson		23 April 2014
Twelves Company (Dorset SARC)	Manager	Michelle Challiss		1 May 2014
Twynham Housing Association	Chief Executive	Marion Franks	To Be Added	July 2008
West Dorset District Council	Chief Executive	David Clarke		10 April 2008
Weymouth & Portland Borough Council	Chief Executive	Tom Grainger		10 April 2008

ORGANISATION	POST	NAME	SIGNATURE	DATE
Weymouth & Portland Housing Ltd	Managing Director	Kevin Dey		18 July 2008
Wiltshire College	Principle - CEO	Di Dale		08 April 2013
Yeovil District Hospital NHS Foundation Trust	Medical Director(& Caldicott Guardian)	Dr J. Howes		04 Sept 2013

1. Introduction

1.1 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. The balance between the need to share information in order to provide quality services, protecting privacy and complying with confidentiality requirements is often a difficult one to achieve.

1.2 The legal situation regarding the protection and use of personal information can be unclear. This may lead to information not being available to those who have a genuine need to know, in order for them to carry out their work effectively.

1.3 This Protocol is a best practice guide to help Dorset councils and other organisations working in partnership with them, to ensure compliance with the law. It does not have any legal standing, nor does it extend or alter the existing legal framework that governs the use and sharing of personal information.

1.4 For the purpose of this Protocol, the terms "data" and "information" are synonymous.

2. Strategic Purpose of the Protocol

2.1 The strategic purpose of this Protocol is to promote the:

(a) delivery of integrated public sector services in line with government initiatives and public expectations; and

(b) the management and planning of cost effective and efficient services.

3. Aims and Objectives

3.1 This Protocol aims to provide Dorset local authorities with a robust framework for the lawful, secure and confidential sharing of personal information between themselves and other public, private or voluntary sector organisations that they work, or wish to work in partnership with. It will enable all partner organisations to meet their statutory obligations and the expectations of the people they serve.

3.2 The objectives of this Protocol are to:

(a) identify the lawful basis for information sharing;

(b) provide guidance on the legal requirements associated with information sharing;

(c) increase awareness and understanding of the key issues involved;

(d) emphasise the need to develop and use Personal Data Exchange Agreements (PDEAs);

(e) explain security requirements relating to the sharing of information;

(f) encourage flows of data;

(g) support a process, which will monitor and review all data flows; and

(h) protect partner organisations from accusations of unlawful use of personal data.

4. Scope

4.1 For the purposes of this Protocol, the terms *personal information* and *personal data* are synonymous.

4.2 This Protocol applies to all personal information processed by partner organisations that will be shared as a result of partnership arrangements under this Protocol.

4.3 The term 'personal information' refers to any information held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that information.

4.4 The Data Protection Act 1998 (DPA) defines personal data as:

"… data which relate to a living individual who can be identified -

(a) from those data; or

(b) from those data and any other information which is in the possession of, or is likely to come into the possession of the data controller [the person or organisation processing that information],

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

4.5 Processing is defined as collecting, obtaining, recording, organising, holding, retrieving, altering, destroying or disclosing data.

4.6 The DPA further defines certain classes of personal information as 'sensitive data', additional conditions must be met for that information to be used and disclosed lawfully, (see Appendix 4).

4.7 This Protocol applies to Elected Members and all employees of the councils or partner organisations, who are involved in partnership working arrangements under this Protocol. It also applies to anyone working in a voluntary capacity within those arrangements.

5. General Responsibilities of Partner Organisations

5.1 By becoming a partner to this Protocol, all organisations are making a commitment to:

(a) adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998 and other associated privacy legislation; and

(b) develop and agree PDEAs detailing the data sharing arrangements for specific, individual information sharing initiatives between partner organisations.

5.2 They will be expected to promote staff awareness of the requirements of information sharing and will be supported by the production of appropriate guidelines where required.

6. Personal Data Exchange Agreements (PDEAs)

6.1 This Protocol serves as the overarching framework to enable the legal and secure exchange of personal information between partner organisations that have a common obligation or desire to provide services within the community.

6.2 Individual PDEAs, as prescribed by this Protocol, will be developed and agreed by participating organisations that need to share personal information to provide services.

6.3 A sample PDEA is attached at Appendix 7.

6.4 All partner organisations that are party to this Protocol will ensure that any PDEA contains:

(a) The purpose(s) for the sharing of personal information.

(b) The legislative basis for the sharing of personal information.

(c) Full details of the organisations that are party to the PDEA.

(d) A nominated lead person for information sharing in each organisation.

(e) The types of personal information that will be shared.

(f) Details of any other organisations with whom personal information may also be shared by the recipient.

6.5 PDEAs will be approved by the respective nominated lead person within each partner organisation participating in the specific information sharing initiative.

6.6 Where information-sharing protocols between organisations exist prior to signing up to this Protocol, such protocols will remain valid. However, these protocols should be reviewed and if necessary brought into line with this Protocol at the earliest opportunity in order to maintain a consistent approach.

6.7 The following are examples of major overarching information sharing protocols which are currently in existence:

(a) Dorset, Poole & Bournemouth Crime & Disorder Partnerships Joint Protocol on Information Exchange.

(b) Bournemouth, Dorset & Poole Multi-Organisation & Information Sharing Protocol (under the Children & Young People's Strategic Partnerships initiative - May 2004).

7. Conditions for Sharing Information

7.1 All partner organisations to this Protocol agree that they may only share information with one another providing the following conditions are met:

(a) the legal basis for sharing information has been established;

(b) the purpose and necessity to share information has been agreed by all parties;

(c) the sharing of information is proportionate to meet the purpose. This will be a matter of professional judgement (appendices 1 & 5 provide guidance only).

8. Recording disclosure / receipt of information

8.1 All partner organisations should have systems in place to record disclosures and receipt of information shared under a PDEA. This will:

(a) create an audit trail to identify wrongful or excessive sharing of information;

(b) allow partner organisations to inform each other whenever information is identified as being inaccurate, misleading or disputed, so that all instances can be corrected, destroyed, clarified or annotated as appropriate; and

(c) facilitate periodic retrospective assessment to be made of whether the information sharing achieved its objectives and where it is determined that it failed to do so, the information sharing should cease or be modified as appropriate.

(d) enable partner organisations to meet their obligations with respect to subject access requests which (unless an exemption applies) include informing the individual of the source of information and details of to whom it has been disclosed.

8.2 In many instances, this will simply be a matter of recording the fact on the file / record. However, particular care should be taken to record instances where sensitive personal information is shared without consent.

8.3 Any requests to disclose information in such circumstances and the disclosures in response to these requests should be documented. A specimen Disclosure Request / Record of Disclosure form can be found at Appendix 11.

8.4 Care should also be taken to ensure that any information sharing which occurs during multi-agency or partnership meetings is recorded.

8.5 It is best practice to adopt and use an information sharing notice and attendance sheet on such occasions. A specimen document can be found at Appendix 10.

9. The Legal Position in Respect of Information Sharing

9.1 <u>The Legal Framework</u>

The principal legislation concerning the protection and use of personal information is:

(a) Data Protection Act 1998.

(b) Human Rights Act 1998 (Article 8).

(c) The Common Law Duty of Confidence.

Other legislation may be relevant when sharing specific types of information.

9.2 <u>Legal powers to share information</u>

9.2.1 Local authorities are able to provide services, collect revenue and undertake a wide range of functions because they are authorised to do so either expressly or implicitly by statute. In view of this any sharing of information that is not authorised by statute would be unlawful.

9.2.2 Therefore, a legislative basis must be identified prior to any sharing of information within a partnership arrangement.

9.2.3 Appendix 2 identifies some of the relevant legislation that facilitates the lawful sharing of information. The legislation listed is not definitive, but represents the most likely to apply to partnership arrangements involving Dorset local authorities and partner organisations.

9.3 The Data Protection Act 1998

9.3.1 The Data Protection Act 1998 governs the protection and use of personal information relating to living individuals.

9.3.2 Any organisation processing personal information is responsible for abiding by the data protection principles and may be under a legal obligation to notify the Information Commissioner of that processing.

9.3.3 Although primarily concerned with protecting personal information, the Act recognises the need to share personal information in certain circumstances. It therefore contains provisions which permit the sharing of such information in certain situations. Appendix 3 sets out these conditions in more detail.

9.4 The Human Rights Act – Article 8

9.4.1 Article 8.1 states that:

"Everyone has a right to respect for his private and family life, his home and his correspondence"

9.4.2 However, this right is not absolute. Article 8.2 acknowledges that under certain conditions, this right can lawfully be overridden.

9.4.3 Appendix 5 sets out these conditions in more detail.

9.5 The Common Law Duty of Confidentiality

9.5.1 Information has a necessary quality of confidence when it is of a confidential character. This does not mean that the information need be particularly sensitive, but simply that it must not be publicly or generally available. For personal information to have the necessary quality of confidence it:

(a) Is not in the public domain or readily available from another source;

(b) Has a degree of sensitivity; and

(c) Is communicated for a limited purpose and in circumstances where the individual is likely to assume an obligation of confidence, e.g. health practitioner/patient, banker/customer, solicitor/client, etc.

9.5.2 The Common Law duty of Confidentiality requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to.

9.5.3 This duty extends to deceased persons as well as living individuals.

9.5.4 Where such a duty exists, it is not absolute. It can lawfully be overridden if the holder of the information can justify disclosure as being in the public interest.

9.5.5 Appendix 5 explains this in more detail.

10. The Use of Non-Personal or Depersonalised Information

10.1 Non-personal or depersonalised information is not covered by the DPA, HRA (Article 8) or the common law duty of confidentiality, as these all relate to personal information.

10.2 In view of this, non-personal or depersonalised information can be lawfully shared. However, you must ensure that the information is in a form where the identity of the individual cannot be recognised i.e. that:

(a) any reference to information that could lead to an individual being identified has been removed; and

(b) the information cannot be combined with any other sources of information held by Partner organisations to produce personal identifiable data.

10.3 Non-personal or depersonalised data should be used wherever possible. It is a breach of the HRA (Article 8) to use personal data when non-personal or depersonalised data would serve the same purpose.

11. Notification Requirements of Partner Organisations

11.1 All partner Organisations are responsible for ensuring that their DPA notification to the Information Commissioner covers the information sharing arrangements established under this Protocol and any associated PDEAs.

12. General Principles Governing the Disclosure of Personal Information

12.1 Partner organisations must ensure that all staff involved in the sharing of personal information under this Protocol, possess the knowledge and authority to take responsibility for making such disclosures.

12.2 This is particularly important where the disclosure of *sensitive personal* information takes place without consent within health and social care organisations. It is generally accepted as good practice that the person involved in such decisions within health and social care organisations will be the Caldicott Guardian.

12.3 The sharing of personal information without either statutory justification, or the consent of the individual concerned places partner organisations and members of staff at risk of prosecution.

12.4 The disclosure of personal information under this Protocol must be:

(a) for a specific, lawful purpose;

(b) absolutely necessary to meet the purpose;

(c) the minimum necessary to meet the purpose;

(d) on a 'need to know' only basis. This Protocol does not give license for unrestricted access to personal information held by another partner organisation;

(e) to identified, authorised persons within the partner organisations; and

(f) recorded by both the providing and receiving partner organisations.

12.5 Adherence to these general principles meets the requirements of the DPA and also satisfies some of the key requirements of the Caldicott principles.

12.6 The Caldicott principles are not a statutory requirement; however National Health Service and social care organisations are committed to them when considering whether confidential information can be shared.

12.7 An information sharing checklist detailing some of the key considerations when sharing personal information is attached at Appendix 1.

13. Consent

13.1 Disclosing information without consent

13.1.1 Consent is not the only means by which personal information can lawfully be disclosed. HRA, DPA and common law all permit personal information to be disclosed without consent under certain circumstances. These circumstances can be summarised as follows:

13.1.2 Data Protection Act 1998:

(a) in the case of non-sensitive personal information, an alternative Schedule 2 condition is met; or

(b) in the case of sensitive personal information, an alternative Schedule 2 **AND** an alternative Schedule 3 condition are met: and

(c) the 'fair processing' provisions of the Act are met. i.e. that the processing concords with what the individual has been told or what they can reasonably expect; or

(d) a relevant exemption under the Act applies. Many of the exemptions are subject to a test of prejudice. Where it is unlikely that advising an individual that you intend to share their personal information would give rise to prejudice, then the fair processing provisions must still be met.

13.1.3 Schedule 2 conditions, schedule 3 conditions and fair processing provisions are detailed in Appendix 4.

13.1.4 For further information on exemptions available under DPA, see Appendix 6.

13.1.5 Human Rights Act- Article 8

(a) the information has no connection with and cannot impact on the private life of the individual; or

(b) it is in accordance with the law; and

(c) it is necessary in a democratic society; and

(d) it is for a legitimate aim; and

(e) it is proportionate.

13.1.6 Common Law Duty of Confidentiality

(a) the information does not have the necessary quality of confidence (see 8.5); or

(b) there is a statutory obligation to disclose; or

(c) disclosure is justified as being in the public interest.

13.2 Obtaining Consent

13.2.1 Partner organisations may choose to obtain consent even when it is not absolutely necessary. This will often represent best practice and it provides a sound basis for the sharing of sensitive personal information. Many of the difficulties in achieving compliance with the legislation can be resolved if the consent of an individual has been obtained.

13.2.2 Where consent is required, or considered to be desirable, partner organisations will obtain it from the individual at the earliest opportunity.

13.2.3 A sample consent form is attached at Appendix 8.

13.3 What is Consent?

13.3.1 For consent to be valid the individual concerned must:

(a) Possess the capacity to give consent.

(b) have received sufficient information to make an informed decision, which includes:

(i) The nature of the information which may be shared.

(ii) Who it may be shared with.

(iii) The purpose, or purposes, for which it will be shared.

(iv) Any other relevant details.

(c) not be acting under duress, i.e. consent must be voluntarily and freely given without any pressure or undue influence.

13.4 Capacity to give consent

13.4.1 In order for an individual to possess the capacity to give consent, they must be capable of retaining, understanding and assessing information material to making that decision.

13.4.2 People under sixteen are capable of giving consent, provided that they are judged to be of sufficient age and maturity to have a general understanding of the nature of what they are being asked to consent to. Obviously some will reach sufficient maturity earlier than others and each case must be assessed individually.

13.4.3 The consent of a parent should be sought if the young person is judged to be incapable of giving consent.[1]

13.4.4 However, even when it is not necessary, parent(s) should be involved in the consent process wherever possible, unless this is against the wishes of the young person.

13.4.5 An individual may lack the mental capacity to give consent. Where another person has been granted a lasting power of attorney or has been appointed to act on their behalf by an order of the Court of Protection, that person should be asked to give consent on behalf of the individual.

[1] Part 1, Sections 2, 3 & 4 of the Children Act 1989 defines persons who may have parental responsibility.

13.4.6 Where no such authority exists and depending on the circumstances, it may be necessary to seek consent from an "appropriate person", such as next of kin or carer.

13.5 Implied or Explicit Consent?

13.5.1 Implied consent may be acceptable where for example, it is clear from an action somebody takes, such as signing up for a particular service, that they agree to the collection / disclosure of personal information to enable the delivery of that service.

13.5.2 Explicit or written consent is preferable where sensitive personal data is to be shared. If this is not possible non-verbal or oral consent should be recorded and witnessed.

13.6 Duration of Consent

13.6.1 In general, once a person has given consent, that consent may remain valid for an indefinite duration for the purposes as defined by the PDEA. If the purpose of the specific partnership significantly changes it may be necessary to seek fresh consent.

13.7 Restrictions on consent

13.7.1 Partner organisations will, as a matter of good practice, seek fresh consent if there are significant changes in the circumstances of the individual or the work being undertaken with them.

13.7.2 A person, having given consent, is entitled at any time to subsequently withdraw that consent or to place restrictions upon the personal information that may be shared. Their wishes must be respected unless there are sound legal reasons for not doing so.

13.7.3 In the event of a person making a request to withdraw or place restrictions on consent previously given, the agency receiving such a request will at the earliest opportunity inform all other partner organisations that may be affected. Details will be recorded by the receiving organisations.

13.8 Refusal of Consent

13.8.1 Where an individual has refused consent and no other lawful reason for processing exists, their personal information must not be shared. Details of the refusal will be recorded by the relevant organisation.

13.8.2 In such circumstances, the individual should be made aware that the level of the service they receive may be adversely affected as a result of their decision, but no undue pressure should be applied to obtain consent.

14. Access Rights

14.1 Under section 7 of the DPA, individuals have a right of access to personal information held about them, subject to any relevant exemptions which may apply.

14.2 Information provided by a partner organisation under this overarching Protocol and an associated PDEA may be disclosed to the individual without the need to obtain the provider's consent. However, a partner organisation will consult with the provider if they have any concerns and in particular if:

(a) The provider has previously stated that the information supplied is subject to an exemption and therefore should not be disclosed to the individual.

(b) The partner organisation is not sure whether an exemption applies.

(c) A Health Practitioner has supplied the information.

(d) Any exemptions under the DPA may apply to the information provided, e.g. prevention and detection of crime, legal professional privilege, health and safety of staff, etc.

14.3 Where two or more partner organisations having a joint (single) record on an individual, that individual may make their request for access to any of the partner organisations. In such cases, the organisation receiving the request will be responsible for processing the request to the whole record and not just the part that they may have contributed, subject to the conditions detailed above.

15. Security and Retention of Information

15.1 Each party to the OAISP will have appropriate policies and procedures covering the security, storage, retention and destruction of personal information.

15.2 For the purposes of information sharing under this Protocol, each Partner organisation will ensure that the transfer or transmission of personal information is via secure means.

15.3 A checklist detailing some 'safe haven' procedures to ensure the secure handling and transfer of personal information is at Appendix 9.

16. Staff Training & Awareness

16.1 All partner organisations will be expected to promote staff awareness of the legal requirements of information sharing. This should be supported by the production of appropriate guidelines where required, which will be made available to all staff via partner organisation Intranet sites and/or via other suitable means of communication.

17. Review of OAISP and PDEAs

17.1 The Dorset Information Management and Compliance Working Group will review this Over Arching Information Sharing Protocol annually.

17.2 In addition to this annual review, any party to the Protocol can request an extraordinary review, at any time, should they consider it necessary.

17.3 Reasons to request an extraordinary review may include the publication of new guidance, legal precedents (both domestic and European), the amendment of existing legislation or implementation of any new legislation as it is enacted.

17.4 Every effort will be made to update this protocol to reflect any changes required by any of the above, as soon as practicable.

17.5 All PDEAs will specify a regular review period, typically an annual occurrence, but this may be shorter or longer depending on the nature of the partnership working taking place.

17.6 Additionally, any party to a PDEA can request an extraordinary review at any time should they consider it necessary.

17.7 Reasons to request an extraordinary review of a PDEA may include significant changes in the nature of the partnership working or service delivery.

17.8 If during the course of a review of this OAISP or any PDEA, it becomes evident that changes are required, all the parties to the relevant agreements will be informed of the fact. All partner organisations will provide assistance in identifying and implementing any necessary amendments.

18. Monitoring PDEAs

18.1 All parties must implement systems capable of monitoring the operation of individual PDEAs in which they are involved. This will facilitate periodic retrospective assessment to be made of whether the information sharing achieves its objectives and where it is determined that it failed to do so, the information sharing should cease or be modified as appropriate

18.2 Therefore Partners to a PDEA should be capable of identifying and logging the following types of incidents:

(a) A refusal by a partner organisation to disclose information when requested;

(b) Conditions being placed on disclosure;

(c) Delays in responding to requests;

(d) Disclosure of information to members of staff who do not have a legitimate reason for access;

(e) Inappropriate or inadequate use of procedures e.g. insufficient information provided;

(f) The use of information for purposes other than those agreed;

(g) Inadequate security arrangements;

(h) Any actual or attempted security breach by an external party (e.g. hacking);

(i) Subject access requests; and

(j) Any actions or omissions, which staff consider to be a breach of the OAISP, individual PDEA or any relevant legislation.

19. Complaints Procedures

19.1 Parties to this Protocol will ensure that they have appropriate complaints procedures in place, relating to the collection, use and disclosure of an individual's personal information.

19.2 In the event of a complaint regarding the disclosure or use of personal information that has been supplied / obtained under a PDEA, all parties to the agreement will provide cooperation and assistance in the investigation and resolution of the complaint.

20. Appendices

1. Information Sharing Checklist.
2. Is Information Sharing Lawful?

3. Is Information Sharing Compatible With The DPA?
4. Additional DPA Information.
5. Is Information Sharing Compatible with the HRA and Common Law?
6. Can Information Be Shared Without Consent?
7. Specimen Personal Data Exchange Agreement (PDEA).
8. Specimen Consent Form.
9. Safe Haven Procedures for the Secure Handling of Personal Information.
10. Specimen Information Sharing Notice and Attendance Record Request.
11. Specimen Disclosure Request / Record of Disclosure.

Appendix 1

Information Sharing Checklist

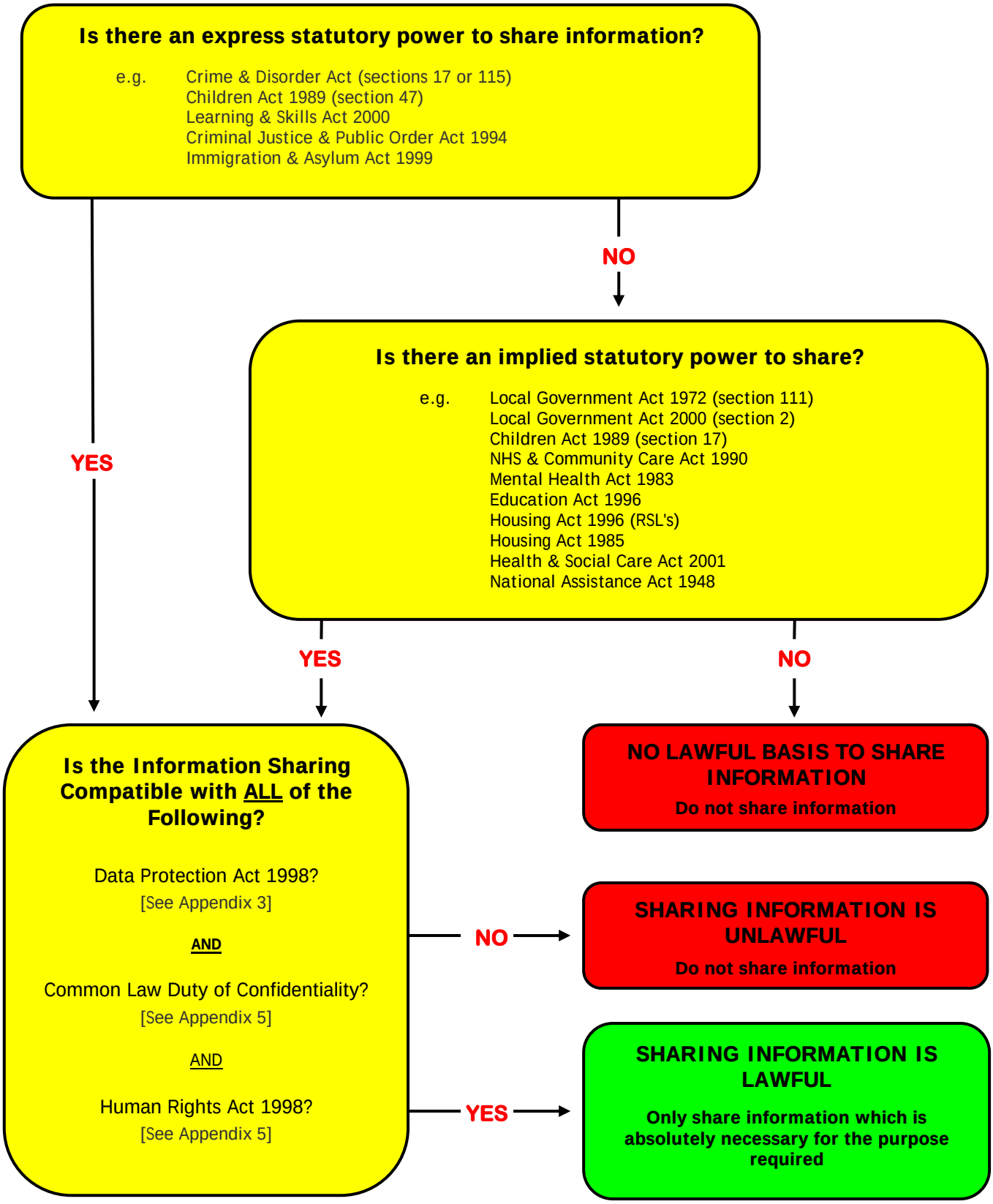
This short checklist will help you to satisfy yourself that any sharing of information you wish to participate in is lawful.

- ☐ Is sharing this information in the best interests of the individual?
- ☐ Is there sufficient need to know i.e. if the information is not shared, would the service offered to or the outcomes in respect of the individual be adversely affected?
- ☐ Is it the minimum amount of information required for the purpose for which it is required?
- ☐ Is the information required to allow one or more of the partner organisations to fulfil their statutory functions?
- ☐ Am I satisfied that the information will be held securely and that only authorised people will have access to it?
- ☐ Am I confident that the personal information is accurate and up to date?
- ☐ Does the information clearly distinguish between fact and opinion or judgement?
- ☐ Will it involve secondary disclosure and if so, am I confident that it will be lawful?
- ☐ Are there any restrictions to consent relating to the use of the information clearly recorded?
- ☐ If consent is not required or cannot realistically be obtained or sought, is there justification for sharing without consent? For example is it necessary to carry out a statutory duty conferred on any organisations in the partnership, or to prevent serious harm, etc.
- ☐ Have I recorded that I have shared this information?
- ☐ Is the information being shared in a secure way?
- ☐ Have details of the information being shared been recorded?

If after going through the checklist, you have any doubts about the whether the proposed information sharing is lawful, you should seek advice from your line manager or the person with responsibility for data protection within your organisation.

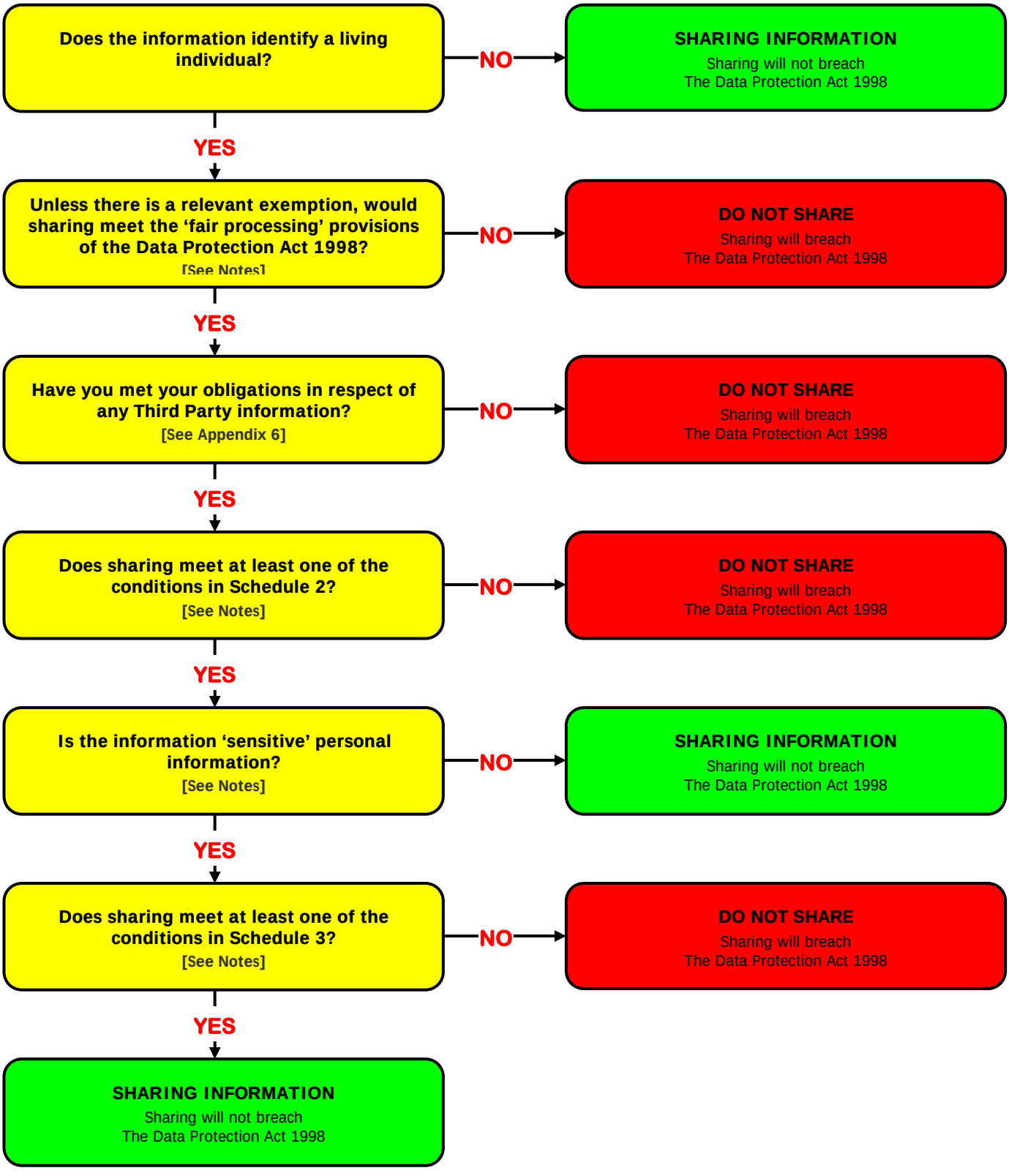
Appendix 2

Is Information Sharing Lawful?



Appendix 3

Is Information Sharing Compatible with the DPA?



Appendix 4 – Additional DPA Information.

Schedule 2 Conditions

One of the following conditions must apply:

1. The individual has consented to the processing ;
2. (a) The processing is necessary for the performance of a contract to which the individual is a party; or

   (b) In response to a request by the individual to enter into such a contract.
3. To fulfil any legal obligation, other than that imposed by contract.
4. To protect the vital interests of the individual, i.e. to protect life or to prevent significant physical / mental harm to the individual or any other person.
5. The processing is necessary –

   (a) for the administration of justice;

   (b) for the exercise of any functions conferred on any person by or under any enactment;

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. For the purposes of the legitimate interests of the organisation holding the information or of the partner organisation to whom it is disclosed but only if those interests do not prejudice the rights and freedoms or legitimate interests of the individual. The Secretary of State may by order, specify particular circumstances in which this condition will or will not apply.

Schedule 3 Conditions

In the case of sensitive personal data, as well as satisfying one of the conditions in Schedule 2, at least one of the following conditions must also apply:

1. The individual has given explicit consent.
2. It is necessary for exercising or performing any right or obligation which is conferred or imposed by law in connection with employment. The Secretary of State may by order, specify circumstances in which this condition does not apply or the circumstances in which additional conditions must be met.
3. To protect a persons vital interests i.e. to protect life or to prevent significant mental / physical harm to the individual or any other person. This condition applies where consent could not reasonably be obtained, or where it is unreasonably withheld, against another persons vital interests.
4. Processing is part of the legitimate activities of a non-profit organisation for political, philosophical, religious or trade union purposes and is carried out with appropriate safeguards for the rights and freedoms of individuals. This condition only applies where the personal information relates to those who are either members of the organisation or have regular contact with it and does not involve disclosing information without the individuals consent;
5. The individual has deliberately caused the information to be made public.

6. Processing is necessary for current or prospective legal proceedings, necessary to obtain legal advice or for establishing, exercising or defending legal rights.
7. Necessary for the administration of Justice, the exercise of any functions conferred on any person by or under an enactment or in the exercise of any function of the Crown, a Minister of the Crown or a government department. The Secretary of State may by order, specify circumstances in which this condition does not apply or the circumstances in which additional conditions must be met.
8. Necessary for medical purposes and is undertaken by a health professional or someone with an equivalent duty of confidentiality.
9. Processing is necessary for the recording of racial or ethnic origin and is necessary for the monitoring and promotion of equal opportunities for racial and ethnic groups. Such processing must be carried out with appropriate safeguards for the individual's rights and freedoms.

Fair Processing Provisions

To comply with the 1st principle of the Data Protection Act individuals must be informed of:

1. Who is responsible for their personal information (who the Data Controller is);
2. The purpose or purposes for which their information will be used; and
3. Who their information may be shared with.
4. Any further information required to allow the individual to fully understand the processing being undertaken and any possible consequences which may result from any information sharing which may take place.

Sensitive Data

Sensitive data is defined as:

- Racial or ethnic origin.
- Political opinions / affiliations.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual orientation or activity.
- Whether they have carried out or been accused of committing any offence.
- Details of court proceedings for any offence committed or alleged to have been committed.
- The disposal of such proceedings or the sentence of any court in such proceedings.

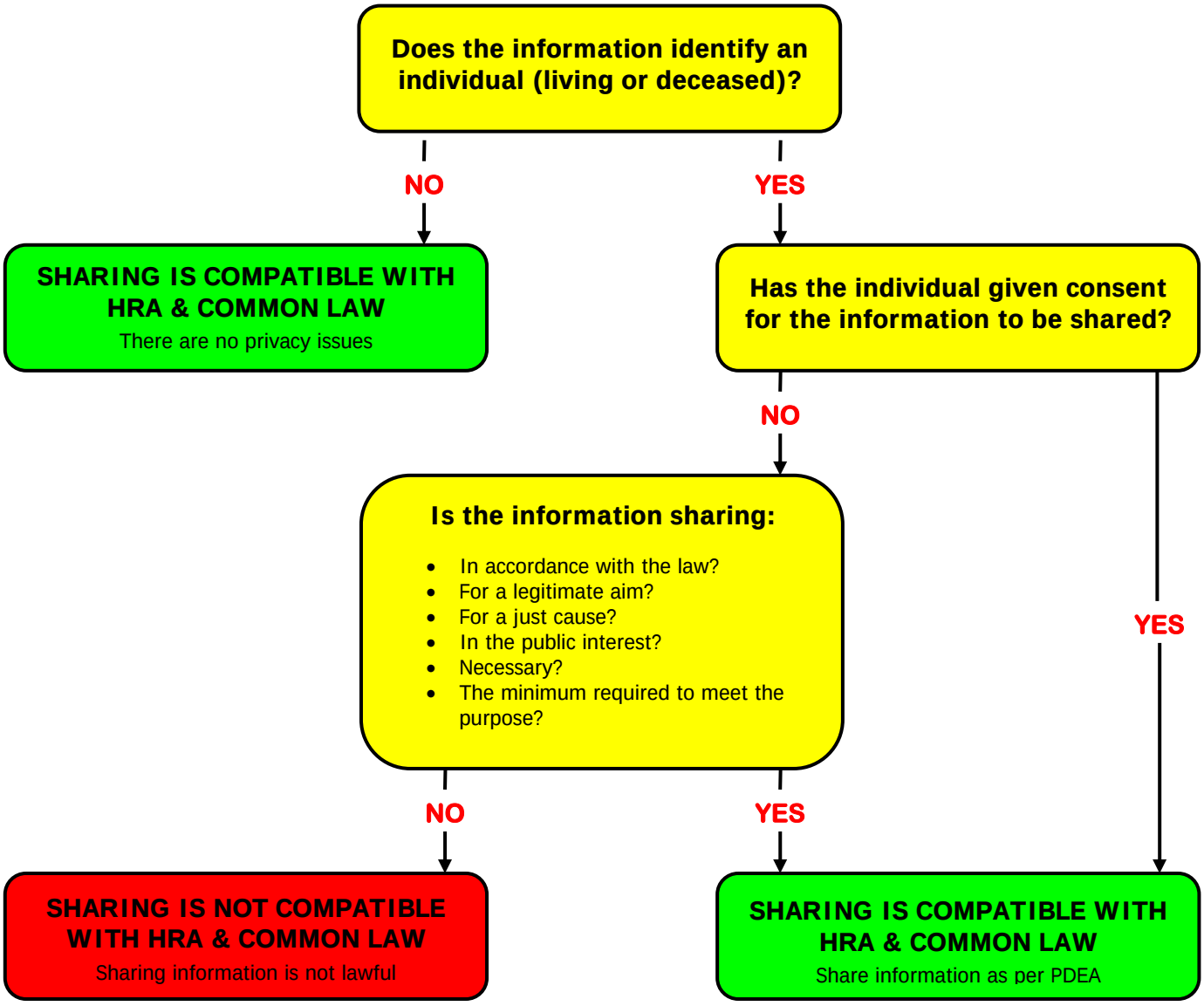
The Data Protection Principles

The rules for processing personal information are known as the 8 data protection principles; these are that information must be:

1. lawfully and fairly processed;
2. not processed for incompatible purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept for longer than is necessary;
6. processed in line with an individuals rights;
7. secure; and
8. not transferred to countries without adequate protection.

Appendix 5

Is Sharing Compatible With HRA & Common Law?

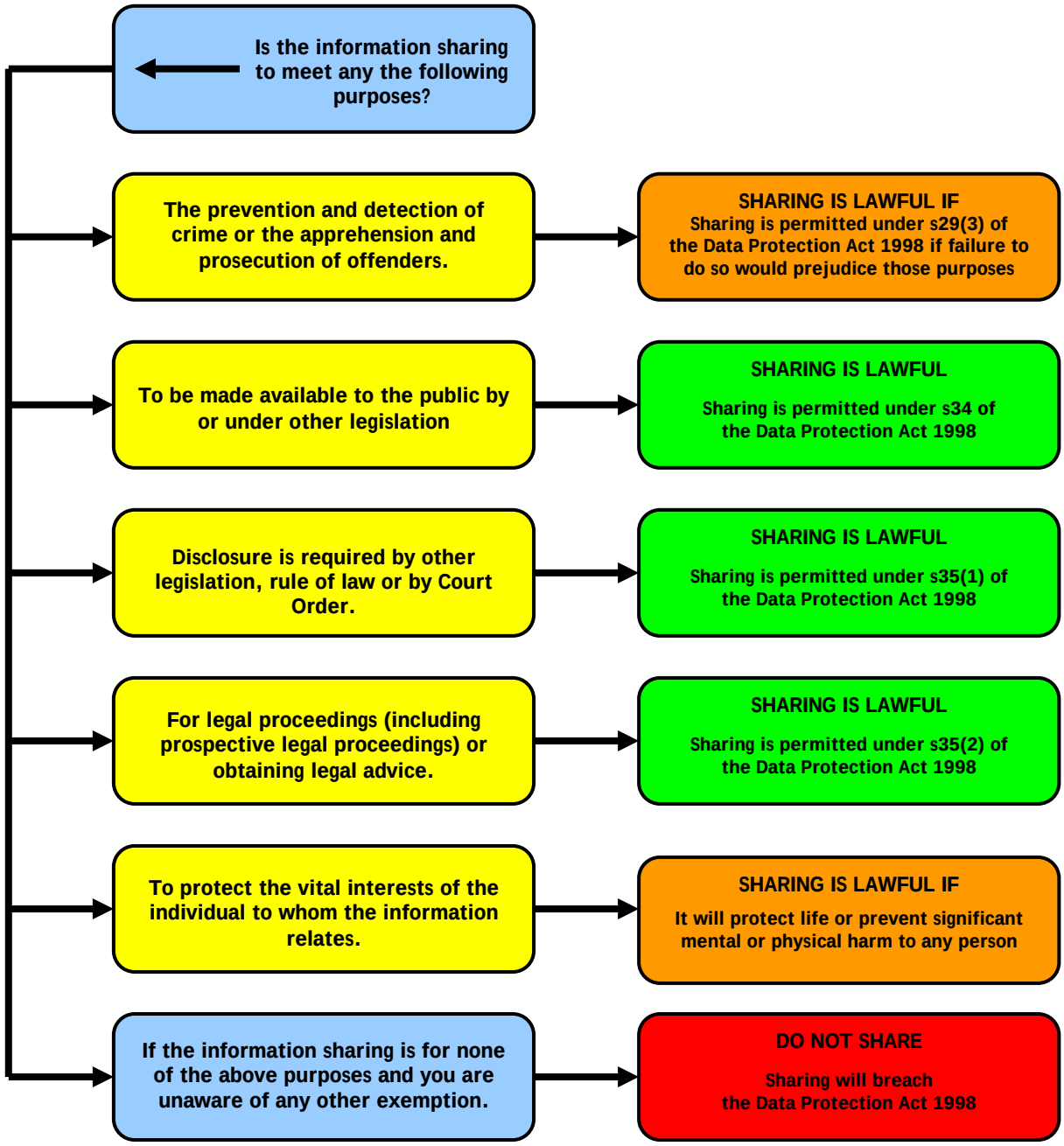


Public Interest criteria include:

- The administration of justice.
- Maintaining public safety.
- The detection and prevention of crime and disorder.
- The apprehension of offenders.
- The protection of vulnerable persons.

Appendix 6

Can Information Be Shared Without Consent?



Note:
The exemptions contained in this flowchart are those that you are most likely to come across but there are others.

There is a degree of overlap between the DPA, HRA and common law duty (tort) of confidentiality. If you have established that the information sharing activity falls within one of the DPA exemptions, it is likely that you will also meet HRA (Article 8) and common law duty of confidentiality requirements.

Appendix 7 - Specimen Personal Data Exchange Agreement (PDEA)

1. Introduction

This PDEA is made under **[**name of the over-arching Information Sharing Protocol that applies**]**.

For example:

(i) *The Dorset, Bournemouth & Poole Crime & Disorder Partnership Joint Protocol on Information Exchange;*

(ii) *The Bournemouth, Dorset & Poole Children & Young People Strategic Partnerships Multi-Organisation Data & Information Sharing Protocol;*

(iii) *Bournemouth, Dorset & Poole Multi-Organisation & Information Sharing Protocol (under the Children & Young People's Strategic Partnerships initiative - May 2004), or*

(iv) *The Bournemouth, Dorset and Poole Over-Arching Information Sharing Protocol (OAISP).*

between:

[Names of organisations involved in partnership working under the agreement**]**.

Note:
Organisations who are signing up to the PDEA must also be signatories to one of the over-arching information sharing protocols as detailed above.

2. Purpose of the PDEA

[Statement clearly defining the purpose(s) for the sharing of personal information. The statement should explain why there is a need to share information between organisations that are party to the agreement**]**.

For example:

- *To safeguard and promote the welfare of vulnerable children who have been identified as causing concern and who have been, or are at risk of being, excluded from school.*
- *To reduce the risk of crime & public disorder by children & young people identified as prolific, priority offenders (PPOs).*
- *To reduce offences, nuisance and hazards of abandoned motor vehicles, and 'communal' vehicles.*

3. Lawful basis for the sharing of personal information

[Details of the legislation that provides the statutory powers (express or implied) for the Council and Partner Organisations to share personal information**]**.

For example:

- *Crime & Disorder Act 1998*
- *Children Act 1989*
- *Education Act 1996*

Note:
Whilst more than one piece of legislation may support the general information sharing framework, the purpose of the PDEA is to clearly define specific, local information sharing initiatives. In view of this, the statutory powers to share information under the PDEA should ideally be confined to one 'key' piece of legislation.

4. Type of personal information that will be routinely shared

[Provide details of the broad categories of personal information to be routinely shared under the agreement**]**.

For example:

- *Personal details - name, address & DOB*
- *Employment details*
- *Financial details*
- *Family, lifestyle and social circumstances*

- *Criminal offences, or alleged offences*
- *Physical or mental health or condition*
- *Sexual life*
- *Racial or ethnic origin*

} *Classified as sensitive personal information under the DPA*

Note:
A combination of categories of personal information may apply under the PDEA.

5. How personal information will be shared

[Statement defining the method(s) that will be used to effect the:

- safe and secure exchange of personal information between agencies, including where applicable the identification of officers within each organisation who are authorised to disclose and receive personal information under the PDEA.
- availability of requested personal information.
- recording of requests for, and disclosures of, personal information**]**.

For example:

- *Personal information must be requested in writing using the agreed proforma.*
- *Personal information may be requested by telephone, fax, or in writing.*
- *Personal information will only be disclosed by a nominated, named officer.*
- *Personal information will be disclosed by officers of the (name of Team, Unit, Section, etc.), who will all be considered to be authorised officers for the purposes of the PDEA.*
- *Responses to requests for information will be effected within (x) days of receipt.*
- *A written record will be maintained of all requests for, and disclosures of, personal information, including requests that have been refused.*

6. Restrictions on the use of shared personal information

[If one of the agencies to the PDEA needs, or wishes to place specific additional restrictions on the use of personal information, these should be indicated in this section of the agreement**]**.

7. Breaches of confidentiality

[Statement defining how breaches of confidentiality by any agencies party to the agreement will be monitored and dealt with**]**.

8. Review of PDEA

[Who will review the PDEA and how often**]**.

9. Termination of PDEA by an organisation

[Statement defining the method by which agencies can terminate their involvement in the PDEA and the length of notice required**]**.

10. Signatories to the PDEA

Authorised signatories from each organisation should formally accept this agreement by completing the table overleaf:

Signatories to the PDEA

Organisation	Post / Position	Name	Signature	Date

Appendix 8

Information Sharing Consent Form

To be used in conjunction with the Dorset OAISP & PDEAs

Consent To Share Personal Information About			
Title	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other:		
Surname		Address	
Forenames			
Date of Birth (if under 16yrs)			

Worker Responsible For Acquiring Consent			
Name		Position	
Organisation		Location	

Actions Carried Out Prior To Obtaining Consent

I have explained to the person:

- ☐ Why we would like the personal information.
- ☐ Who we will share the information with.
- ☐ Who will have access to the information.
- ☐ Their rights under the Data Protection Act.
- ☐ How long the information will be kept.
- ☐ Their right to withdraw or restrict consent.
- ☐ What information will be shared.
- ☐ The complaints procedure.
- ☐ Why we need to share the information.
- ☐ Who to contact for further information.
- ☐ Possible consequences of any restrictions or refusal of consent.

Any other actions carried out prior to obtaining consent:

Brief Description Of Type Of Information And Purpose Of Sharing

Personal Information Will Or May Be Shared With

- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

Restrictions To Consent

The following restrictions apply to these information sharing arrangements (indicate if none):

Duration Of Consent

☐ As long as required for the purpose(s) as detailed.

☐

Any Other Relevant Details

Declaration

Read this form carefully. If you have **any** concerns, please discuss them with the person who is seeking your consent.

I confirm that I have been informed of the information sharing arrangements as detailed above and that ***I consent** / **do not consent** to those arrangements. I understand that I have the right to withdraw or restrict my consent to these arrangements at any time.

* Delete as appropriate

Signature		**Date**	

Parental Consent Or Alternative Lawful Authority

If the individual is too young or otherwise incapable of giving informed consent, the consent of an appropriate person with lawful authority to act on behalf of the individual should be recorded below.

Title	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other:		
Name		Relationship to individual	

I confirm that I have been informed of the information sharing arrangements in respect of the above named individual as detailed above and that ***I consent** / **do not consent** on their behalf to those arrangements. I understand that I have the right to withdraw or restrict my consent to these arrangements at any time.

* Delete as appropriate

Signature		**Date**	

Witness To Consent (If Unable To Obtain Written Consent)

If the individual is unable to sign but has indicated their consent by other means, an independent witness should sign below to confirm that fact.

Title	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other:
Name	

I confirm that the person named overleaf has indicated that they ***consent / do not consent** to the information sharing arrangements as detailed.

* Delete as appropriate

Signature		**Date**	

Appendix 9 – Safe Haven Procedures for the Secure Handling of Personal Information

Safe Haven procedures in the context of this Protocol cover:

- Fax
- Paper records
- E-mail/computer
- Telephone/Spoken communication
- Post/Informal messages e.g. post-it notes/telephone message notes

Best Practice Checklist

Fax machines

- ☑ Ensure fax equipment is sited where unauthorised people cannot access it.
- ☑ When sending information by fax, do not include customer/client/patient details unless absolutely necessary.
- ☑ Programme numbers into the fax machine memory to avoid misdialling.
- ☑ Confirm the fax number before sending.
- ☑ Check that recipient is waiting to receive a confidential fax.
- ☑ Always use an official fax header with a confidentiality statement printed on it.

Paper records and files

- ☑ All paper records containing personal and/or confidential information must be maintained and handled securely.
- ☑ Effective security must be maintained when personal and/or confidential information is being transferred or taken out of a secure environment.
- ☑ Any loss of personal and/or confidential records must be reported immediately to the officer who has responsibility for information compliance within the organisation/department, e.g. Caldicott Guardian, Information Governance Manager, Data Protection Officer, Unit Information Compliance Officer, etc., and the line manager.

E-mail and computer use

- ☑ Only use electronic mail in accordance with your organisation's policy.
- ☑ Do not send external emails containing confidential and/or personal customer/client/patient information unless suitable encryption facilities are available.
- ☑ Ensure that computer screens showing confidential and/or personal information cannot be seen by unauthorised people.
- ☑ Ensure that passwords are maintained securely, not shared with others and changed regularly.
- ☑ Ensure that all personal customer/client/patient information stored is accurate.
- ☑ Only record information that is relevant and remember that an individual has a right of access to their personal information.

Telephone & verbal communication

- ☑ Check to see whether confidential conversations may be overheard and take steps to ensure that they are not.
- ☑ When discussing confidential information using the telephone you must be confident that the person on the other end should be receiving the information.
- ☑ Avoid sharing confidential information in public places, e.g. reception counters.

Post, informal messages and notes

- ☑ Check addresses are up to date and ensure that letters are addressed correctly.
- ☑ Always seal envelopes containing confidential information.
- ☑ Destroy in a secure manner, all informal or 'short shelf life' information which is no longer required, e.g. post-it notes, telephone messages.

General

- ☑ Ensure that visitors are not able to access confidential information.
- ☑ All contractors have a contractual obligation to maintain confidentiality, but access to sensitive personal data should be restricted where practicable.
- ☑ Take care when releasing information to relatives, e.g. giving information to separated parents about children.

This list is not definitive, but highlights some areas of best practice. The list may be amended or added to provide a more detailed guide for Partner Organisations.

Appendix 10 -

Information Sharing Notice and Attendance Record For Multi-Agency / Partnership Meetings

Details of Meeting			
Meeting			
Location			
Date		Time	
Lead Agency			
Purpose of Meeting	e.g. meeting the objectives of the Crime, Drugs & Disorder Strategy		
Lawful Basis For Sharing Information	e.g. Section 115 of the Crime and Disorder Act 1998		
Any Other Relevant Information			

Confidentiality Notice

We, as signed overleaf, understand that personal information sharing at this meeting is for the purpose stated above. The lawful basis for such information sharing is [state legislative basis, e.g. Section 115 of the Crime & Disorder Act].

We understand and agree to comply with:

- the information sharing principles as set out in [whichever Information Sharing Protocol and Personal Data Exchange Agreement that apply, e.g. the Bournemouth, Dorset & Poole Over-Arching Information Sharing Protocol and the Prevent & Deter Personal Data Exchange Agreement].
- our obligations under the Data Protection Act 1998, Article 8 of the Human Rights Act 1998 and the common law duty of confidentiality.

We also understand that any personal information shared as part of this meeting, is only to be used for the purpose(s) detailed above and cannot be used for any other purpose(s), unless there is a lawful power to do so.

The minutes / notes of this meeting will serve as a formal record of the personal information that has been exchanged between those present.

Information Sharing And An Individual's Rights Under The Data Protection Act 1998

The Data Protection Act 1998 includes provisions which grant individuals a number of statutory rights. The following are of particular relevance to information sharing:

- Fair processing provisions – which require that an individual is informed about the purpose(s) for which their personal information will be used and who it may be shared with.
- The subject access provisions – which gives individuals a right of access to any recorded personal information that is held about them.
- Non-disclosure provisions – which prevent personal information being disclosed unless the individual has been informed of such disclosure and has consented to it.

In order to comply with these provisions, individuals whose personal information is shared at this meeting, must have been informed about the multi-agency partnership working to which these meetings relate and provided with (or provided access to) the Information Sharing Protocol & Personal Data Exchange Agreement referred to above.

They will normally have a right of access to personal information recorded during this meeting; this includes personal information included in the notes / minutes of this meeting.

However, the Act does contain exemptions to the above provisions. Where information sharing is taking place under an exemption, that fact should be clearly indicated in the notes / minutes.

The most likely exemptions are listed below. If there is any doubt as to whether an exemption applies, the lead agency will seek appropriate advice in order to establish the legal situation.

Most Likely Exemptions Under The Data Protection Act 1998

- Prevention and detection of crime and the apprehension and prosecution of offenders. This exemption must be considered on a 'case by case' basis. Information shared for these purposes is exempt from the fair processing provisions and subject access provisions if complying with them would prejudice that purpose.
- Health, education and social work, where disclosure would be likely to cause serious harm to the physical or mental health or condition of the individual or any other person.
- Disclosures required by law in connection with legal proceedings.
- Legal professional privilege.
- Regulatory functions – this includes securing the health, safety and welfare of employees.
- Third Party Information - there is no obligation to disclose information which would identify an individual who has expressed a desire for confidentiality or where it is reasonable to assume such a desire.
- Third Party Information - there is no obligation to disclose information if it relates to or was supplied by an individual and disclosure would identify that individual and represent a breach of their rights under the Data Protection Act 1998.

  This exemption does not apply to organisations, thus information that would reveal that a particular organisation had supplied information is not exempt, unless disclosure would identify a particular individual. Information is not usually completely withheld in these circumstances, but if possible edited to conceal the identity of the third party.

  Statutory Instruments have been issued, which provide that information which identifies health professionals or social workers acting in their professional capacity should normally be disclosed.

Information Sharing Notice and Attendance Record

For Multi-Agency / Partnership Meetings

Name	Post	Organisation	Signature

Appendix 11

Disclosure Request

To be used when requesting disclosure of personal information without the consent of the individual.

Request From			
		Request Ref.	
Organisation		Location	
Person		Post	
Request To			
Organisation		Location	
Person (If known)		Post (If known)	
Subject Details			
Surname		Address (if Relevant)	
Forenames			
Date of Birth			
Unique Personal Identifier			

Information To Be Disclosed

Purpose for which information is required: (e.g. Child in Need assessment, prevention or detection of crime).

Lawful Basis for Request: (e.g. Specific statute or exemption to the Data Protection Act 1998).

Information Required & Requested Means of Disclosure: (e.g. Fax, Post, By Hand etc.).

If Information is to be Shared Without Consent or After Consent Refused, State Reasons for Doing So.

Any Other Relevant Information: (include name of relevant Personal Data Exchange Agreement).

Declaration

I confirm that the above information is required for the purposes stated. Any obligations arising from the Data Protection Act 1998, Article 8 of the Human Rights Act 1998 or any Common Law Duty of Confidentiality will be observed. The information will not be used for any purpose other than that for which it is being requested and will not be further disclosed to any unauthorised person. It will be kept securely and where necessary, disposed of correctly in accordance with the relevant retention schedule.

Signed		Date	

Record of Disclosure

To be used when disclosing personal information without the consent of the individual.

Request Received By			
Request Ref.		Disclosure Ref.	
Person		Post	
Receipt via		Date Received	

Information Disclosed

Purpose of Information Disclosure: (e.g. Child in Need assessment, prevention or detection of crime).

Lawful Basis for Disclosure: (e.g. Specific statute or exemption to the Data Protection Act 1998).

Information Disclosed:

If Information was Shared Without Consent or After Consent Refused, State Reasons for Doing So.

Means of Disclosure: (including details of person information disclosed to).

Details of Any Differences Between Request and Disclosure:

Reasons for Refusal / Limited Disclosure:

Declaration

I confirm that to my knowledge, the above information is a true record of the information as held by us, that it was obtained fairly and lawfully, and that I am authorised to make the disclosure as detailed above.

Signed		Date	

*** Use continuation sheet if required.**

Disclosure Request

To be used when requesting disclosure of personal information without the consent of the individual.

Continuation Sheet
Any Other Relevant Information: