Appendix A: Slough Wellbeing Board's Overarching Information Sharing Protocol

Document Control

Document details	
Document name	Slough Wellbeing Board's Overarching Information Sharing Protocol
Document version number	*1.0*
Document status	*Live*
Author	*Amanda Renn, Policy Officer, Policy and Communications team*
Lead Officer	*Samantha Jones, Policy Manager, Policy and Communications team*
Approved by	
Scheduled review date	

Version History		
Version	**Change/Reasons for Change**	**Date**
1	*Initial draft*	*March 2015*
2	*(a) Minor changes needed to paragraph 6 of the Protocol and paragraph 7 of the Guidance to reflect Legal Service's advice; and* *(b) Guidance and templates brought into the main body of the Protocol as appendices (and original appendices and annexes renumbered accordingly).*	*April 2015* *April 2015*

Approval history		
Version	**Approving body**	**Date**
2	*Slough Wellbeing Board*	

Slough Wellbeing Board's
Overarching Information Sharing Protocol

April 2015

Slough Wellbeing Board's
Overarching Information Sharing Protocol

Contents

Slough Wellbeing Board's Overarching Information Sharing Protocol

1. Background

Sharing information about individuals between organisations is often essential to keep people safe, or make sure they get the best services.

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.

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.

This Protocol (and its accompanying best practice guide at appendix B) has been developed to ensure that the Slough Wellbeing Board and other organisations working in partnership with it, comply with the law. It describes a common set of principles and defines the general parameters within which each of the signatory organisations that are party to this Protocol will share information with each other.

This Protocol 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.

It does however establish ownership and transparent agreement to the spirit of information sharing in the best interests of service users and their families and carers and commits those who sign up to it to share information lawfully, ethically and effectively at all levels of their organisation or agency.

It also provides the context for the underlying tiers in Slough Wellbeing Board's Information Sharing Framework.

Individual signatory organisations will need to agree individual agreements that deal with more specific issues – e.g. crime and disorder or the sharing of information about children.

These individual agreements will need to refer to, and be compatible with, the requirements of this Protocol.

2. Organisations covered by this Protocol

This Protocol has been developed to meet the information security requirements for sharing information between the partner organisations listed at appendix A.

3. Strategic purpose of this Protocol

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.

4. Aims and objectives of this Protocol

This Protocol aims to provide Slough Wellbeing Board with a robust framework for the lawful, secure and confidential sharing of personal information between Slough Wellbeing Board members 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.

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 (see appendix B);
(c) Increase awareness and understanding of the key issues involved;
(d) Emphasise the need to develop and use individual agreement where appropriate;
(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.

5. Scope

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

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

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.

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".

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

The DPA further defines certain classes of personal information as ‘sensitive data', and additional conditions must be met for that information to be used and disclosed lawfully.

This Protocol applies to Slough Wellbeing Board members, elected members and all employees of the council and 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.

6. General responsibilities of partner organisations

By becoming a partner to this Protocol, partner organisations agree to:

(a) Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998 and other associated privacy legislation;
(b) Adhere to or demonstrate a commitment to achieving the appropriate compliance with any guidance published by the Information Commissioner’s Office; and
(c) Develop and agree agreements detailing the data sharing arrangements for specific, individual information sharing initiatives between partner organisations.

7. Individual agreements

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

Individual agreements prescribed by this Protocol (such as Community Information Agreements (CIA) (tier 2) and Purpose Specific Information Agreements (PSIA) (tier 3) will be developed and agreed by participating organisations that need to share personal information to provide particular services.

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

Where individual agreements already exist between organisations prior to Slough Wellbeing Board members signing up to this Overarching Information Sharing Protocol, these arrangements will remain valid.

However, these agreements will be reviewed and if necessary amended so that they are brought into line with this Protocol at the earliest opportunity in order to maintain a consistent approach.

8. Conditions for sharing information

All organisations party to this Protocol agree that they will only share information with one another if the following conditions can be 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.

9. Recording disclosure / receipt of information

All organisations party to this Protocol will put in place systems to record the disclosure and receipt of information shared under this Protocol and any individual agreement created under it. These 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;
(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; and
(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.

In most instances, this will simply be a matter of recording the fact on the file / record. However, particular care will be taken to record instances where sensitive personal information is shared without consent. Partners will ensure that any requests to disclose information in such circumstances and the disclosures that result in response to these requests are documented using a Disclosure Request / Record of Disclosure form.

Partners will also ensure that any information sharing which occurs during multi-agency or partnership meetings are also recorded using an Information Sharing notice and Attendance sheet.

10. Legal requirements

Under this Protocol, the principal* legislation concerning the protection and use of personal information is:

(a) Data Protection Act 1998 (DPA)
(b) Human Rights Act 1998 (Article 8) (HRA)
(c) The Common Law Duty of Confidence

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

11. The use of non-personal or depersonalised information

Non-personal or depersonalised information is not covered by the DPA, HRA or the common law duty of confidence, as these all relate to personal information. In view of this, non-personal or depersonalised information can be lawfully shared be shared under this Protocol. However, partner organisations will 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.

12. Notification requirements of partner organisations

All partner organisations are responsible for ensuring that their DPA notifications to the Information Commissioner's Office cover the information sharing arrangements established under this Protocol and any associated individual agreements.

13. General principles governing the disclosure of personal information

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

This is particularly important where the disclosure of sensitive personal information takes place without consent within health and social care organisations.

Under the terms of this Protocol it is generally accepted that the person involved in such decisions within health and social care organisations will be their Caldicott Guardian.

The sharing of personal information without statutory justification, or the consent of the individual concerned, can place partner organisations and members of staff at risk of prosecution. In order to reduce this risk, the disclosure of personal information under this Protocol will 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.

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

**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.*

14. Access rights

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. This means that any information provided by a partner organisation under this Protocol (and any individual agreement created under it) may be disclosed to the individual without the need to obtain the provider's consent.

However, the partner organisation will be expected to 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.

Where two or more partner organisations have 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

All organisations party to this Protocol will put in place appropriate policies and procedures covering the security, storage, retention and destruction of personal information.

For the purposes of information sharing under this Protocol, each partner organisation will ensure that:

(a) The transfer or transmission of personal information is via secure means; and
(b) That all requests for information are responded to within a reasonable and realistic time scale.

16. Staff training and awareness

All organisations party to this Protocol will be expected to promote staff awareness of the legal requirements of information sharing. This will be supported by the production of appropriate guidance where required, which will be made available to all staff via their Intranet sites and/or via other suitable means of communication.

They will also ensure that their Designated Officer(s) is widely known within their organisation.

17. Review of this Protocol

Slough Wellbeing Board will review this Protocol annually.

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

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.

Every effort will be made to update this Protocol to reflect any changes required by any of the above, as soon as practicable. Any individual agreements made under this Protocol 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.

Additionally, any party to an individual agreement can request an extraordinary review at any time should they consider it necessary. Reasons to request an extraordinary review of an individual agreement may include significant changes in the nature of the partnership working or service delivery.

If during the course of a review of this Protocol, or any individual agreement made under it, 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

All organisations that are party to this Protocol must implement systems capable of monitoring the operation of any individual agreements in which they are involved. This will allow a periodic retrospective assessment to be made of whether the information sharing arrangements that have been put in place achieve their objectives and where it is determined that they failed to do so, the information sharing arrangements should cease or be modified as appropriate.

All organisations party to this Protocol and any individual agreements created under it will routinely identify and log 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 this Protocol, individual agreements or any relevant legislation.

19. Complaints procedure

All organisations that are party 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.

In the event of a complaint regarding the disclosure or use of personal information that has been supplied / obtained under this Protocol, or any individual agreements made under it, all organisations party to this Protocol or the individual agreement will provide co-operation and assistance in the investigation and resolution of the complaint.

Appendix A: Signatories to the Slough Wellbeing Board Overarching Information Sharing Protocol

This Protocol has been signed by the following Chief Executive (or equivalent) of the respective organisations on behalf of their organisations and their Caldicott Guardians (or Designated Officers).

Organisation	Post/position	Name	Signature	Date

Appendix B: Overarching Information Sharing Protocol: Guidance

April 2015

Slough Wellbeing Board

Overarching Information Sharing Protocol: Guidance

Contents

Annexes

Overarching Information Sharing Protocol Guidance

1. Executive Summary

This guidance summarises the arrangements for inter-agency information sharing in Slough.

It sets out the standards that elected members, council employees and other organisations working in partnership with the Slough Wellbeing Board must adhere to.

It is intended to complement any existing professional codes of practice that apply to any relevant professionals working in or with partner agencies.

2. Introduction

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.

The legal situation regarding the protection and use of personal information can often 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.

This guide has been developed to help elected members, council employees and other organisations working in partnership with the Slough Wellbeing Board, 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.

3. Strategic purpose of this guide

The strategic purpose of this guide 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.

4. Aims and objectives

This guide **aims** to provide elected members, council employees and other organisations working in partnership with the Slough Wellbeing Board 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 elected members, council employees and partner organisations to meet their statutory obligations and the expectations of the people they serve.

The **objectives** of this guide 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 Community Information Agreements (CIA) and Purpose Specific Information Agreements (PSIA) where appropriate;
(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 elected members, council employees and partner organisations from accusations of unlawful use of personal data.

5. Scope

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

This guide applies to all personal information processed by council staff and partner organisations that needs to be shared as a result of partnership arrangements under the Slough Wellbeing Board's Overarching Information Sharing framework.

The term 'personal information' refers to any information that is held manually or electronically, including records held by means of audio and/or visual technology, about an individual who can be personally identified from that information.

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".

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

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.

Annex 4 provides further guidance on this issue.

This guide applies to elected members and all employees of the council and signatories to the Slough Wellbeing Board's Overarching Information Sharing Protocol and who are involved in partnership working arrangements under that Protocol. It also applies to anyone working in a voluntary capacity within those arrangements.

6. Information sharing framework/structure

Slough Wellbeing Board's information sharing framework comprises the following elements:

Tier 1 - Slough Wellbeing Board's Overarching Information Sharing Protocol

This Protocol is a high level policy document common to all organisations delivering health, social and community services across Slough. It describes a common set of **principles** and defines the general parameters within which the signatory organisations that are party to it will share information with each other.

It establishes ownership and transparent agreement to the spirit of information sharing in the best interests of service users and their families and carers, and it commits those who sign it to sharing information lawfully, ethically and effectively at all levels of their organisation. Slough Wellbeing Board's Overarching Information Sharing Protocol also provides the context for each of the underlying tiers in the model (see below).

Slough Wellbeing Board's Overarching Information Sharing Protocol was signed by members the Chief Executives (or their equivalents) and by their Caldicott Guardians (or Designated Officers).

Tier 2 - Community Information Agreements (CIA)

These agreements are high level agreements common to organisations and agencies delivering health, social and community services.

They satisfy the Tier Two level of the Model and focus on the collective **purpose** underlying the sharing of information with the 'information community' and describe common contexts and shared objectives between agencies delivering services of a similar scope.

They reference the relevant underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information within the same information community.

They also provide the context for a supporting set of individual Purpose Specific Information Agreements (PSIA) (Tier 3) (see below), which set out at a detailed level, how personal information can be shared amongst organisations within the same information community.

Community Information Agreements are usually signed by Service Directors or the equivalent functional leads.

Tier 3 - Purpose Specific Information Agreements (PSIA)

These agreements are the lowest level of the three tier model.

They are aimed at an organisation's "operational management/practitioner" level and define the relevant processes which support the information sharing between two or more organisations or agencies for a specified purpose.

These documents capture:

- What information is to be shared
- What it is being shared (for what purpose)
- Who it is being shared with (between organisations and agencies)
- When it is being shared (the times and frequency etc)
- How is it being shared (format)

Purpose Specific Information Agreements are usually signed by Heads of relevant services who have the devolved local and/or operational responsibility for delivery.

7. General responsibilities of partner organisations

By becoming a partner to the Slough Wellbeing Board's Overarching Information Sharing Protocol, signatories 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;
(b) Adhere to or demonstrate a commitment to achieving the appropriate compliance with any guidance published by the Information Commissioner's Office; and
(c) Develop and agree the use of individual Community Information Agreements (CIA) and Purpose Specific Information Agreements ((PSIA) (see section 8 below) that detail the data sharing arrangements for specific, individual information sharing initiatives between partner organisations.
(d) Promote staff awareness of the requirements of information sharing and support by the production of appropriate guidelines where required.

8. Community Information (CIA) and Purpose Specific Information (PSIA) Agreements

Slough Wellbeing Board's Overarching Information Sharing 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.

Individual CIAs and PSIAs, as prescribed by Slough Wellbeing Board's Overarching Information Sharing Protocol, must be developed and agreed by participating organisations that need to share personal information to provide services.

A specimen CIA is attached at annex 11.

A specimen PSIA is attached at annex 12.

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol must ensure that any CIAs or PSIAs developed contain:

(a) The purpose(s) for the sharing of personal information (CIA).
(b) The processes that will be used to support information sharing between two or more organisations or agencies for a specified purpose (PSIA)
(c) The legislative basis for the sharing of personal information.
(d) Full details of the organisations that are party to each CIA or PSIA.
(e) A nominated lead person for information sharing in each organisation.
(f) The types of personal information that will be shared.
(g) Details of any other organisations with whom personal information may also be shared by the recipient.

All CIAs and PSIAs must be approved by the respective nominated lead person within each partner organisation participating in the specific information sharing initiative.

Where information sharing protocols and or agreements between organisations exist prior to members having signed up to Slough Wellbeing Board's Overarching Information Sharing Protocol, such protocols and agreements will remain valid. However, these documents should be reviewed and if necessary brought into line with Slough Wellbeing Board's Overarching Information Sharing Protocol at the earliest opportunity in order to maintain a consistent approach.

9. Conditions for sharing information

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol have agreed that they will only share information with one another if 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.

A flow chart of key questions to ask is at annex 1. Annex 5 also provides additional guidance on this issue.

10. Recording disclosure / receipt of information

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are required to put in place systems that record disclosures of and receipt of information shared under a CIA or PSIA. 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 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.
(c) 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.

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.

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 annex 10.

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

It is best practice to adopt and use information sharing notice and attendance sheet on such occasions. A specimen can be found at annex 9.

11. The legal position in respect of information sharing

Legal framework

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

(a) Data Protection Act 1998 (DPA)
(b) Human Rights Act 1998 (Article 8) (DPA)
(c) The Common Law Duty of Confidence

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

Legal powers to share information

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

Annex 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 the council, the wellbeing board and its partner organisations.

The Data Protection Act 1998

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

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.

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.

Annex 3 explains these conditions in more detail.

The Human Rights Act 1998 – Article 8

Article 8.1 states that: *"Everyone has a right to respect for his private and family life, his home and his correspondence".*

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

Annex 5 explains these conditions in more detail.

The Common Law Duty of Confidentiality

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.

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.

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

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.

Annex 5 explains this in more detail.

12. The use of non-personal or depersonalised information

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. In view of this, non-personal or depersonalised information can be lawfully shared. However, staff 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.

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.

13. Notification requirements of partner organisations

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are responsible for ensuring that their DPA notification to the Information Commissioner covers the information sharing arrangements established under the Overarching Information sharing Protocol and any individual CIAs and PISAs created under it.

14. General principles governing the disclosure of personal information

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are required to ensure that all staff involved in the sharing of personal information under this Protocol possess the relevant knowledge and authority to take responsibility for making such disclosures.

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.

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.

The disclosure of personal information under Slough Wellbeing Board's Overarching Information Sharing Protocol should only occur:

(a) For a specific, lawful purpose;
(b) Where it is absolutely necessary to meet the purpose;
(c) As the minimum necessary to meet the purpose;
(d) On a 'need to know' only basis. Slough Wellbeing Board's Overarching Information Sharing 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.

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

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.

The flow chart of key questions at annex 1 explains some of the key considerations that need to be taken into account when sharing personal information.

15. Consent

Disclosing information without consent

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 are summarised as follows:

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.

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

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

Human Rights Act 1998 - 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.

Common Law Duty of Confidentiality

(a) The information does not have the necessary quality of confidence; or
(b) There is a statutory obligation to disclose; or
(c) Disclosure is justified as being in the public interest.

Obtaining Consent

Signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol 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.

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

A specimen consent form is attached at annex 7.

What is Consent?

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.

Capacity to give consent

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.

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.

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

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.

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.

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.

Implied or explicit consent?

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.

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.

Duration of consent

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

Restrictions on consent

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.

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.

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.

Refusal of Consent

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.

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.

16. Access rights

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.

Information provided by a partner organisation under this overarching Protocol and an associated CIA or PSIA 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.

Where two or more partner organisations have 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.

17. Security and retention of information

Signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol will have appropriate policies and procedures covering the security, storage, retention and destruction of personal information.

For the purposes of information sharing under Slough Wellbeing Board's Overarching Information Sharing Protocol, each partner organisation will ensure that the transfer or transmission of personal information is via secure means.

A checklist explaining some 'safe haven' procedures to ensure the secure handling and transfer of personal information is at annex 8.

18. Staff training and awareness

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are expected to promote staff awareness of the legal requirements of information sharing.

See section 22 for further guidance on this issue.

19. Review of CIAs and PSIAs

Slough Wellbeing Board will review its Overarching Information Sharing Protocol annually. In addition to this annual review, all parties to this Protocol can request an extraordinary review, at any time, should they consider it necessary. 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. Every effort will be made to update this protocol to reflect any changes required by any of the above, as soon as practicable.

All CIAs and PSIAs created under the Overarching Protocol will specify a regular review period, this is typically an annual occurrence, but it may be shorter or longer depending on the nature of the partnership working taking place. Additionally, any party to a CIAs or PSIAs can request an extraordinary review at any time should they consider it necessary. Reasons to request an extraordinary review of a CIAs or PSIAs may include significant changes in the nature of the partnership working or service delivery.

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

20. Monitoring

Partner organisations are expected to implement systems capable of monitoring the operation of individual CIAs and PSIAs in which they are involved. This will enable a periodic retrospective assessment to be made of whether the information sharing arrangements achieve their objectives and where it is determined that they have failed to do so, the information sharing should cease or be modified as appropriate.

All signatories to any CIAs and / or PSIAs created under Slough Wellbeing Board's Overarching Information Sharing Protocol are also required to routinely identify and log 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 Slough Wellbeing Board's Overarching Information Sharing Protocol, individual CIAs or PSIAs and relevant legislation.

21. Complaints procedures

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol will ensure that they have appropriate complaints procedures in place, relating to the collection, use and disclosure of an individual's personal information.

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

22. General information sharing guidance

Data Protection Act 1998 – Guidance for Social Services
Available at
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4010391

Confidentiality: NHS Code of Practice (DH, 2003)
Available at www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

Confidentiality: protecting and providing information (GMC, 2004)
Available at www.gmc-uk.org/guidance/current/library/confidentiality.asp

The NMC Code of Professional Conduct: Standards for Conduct, Performance and Ethics (NMC, 2004)
Available at www.nmc-uk.org

HM Government Information sharing vision statement (HMG, 2006).
Available at www.justice.gov.uk/publications/informationsharingvision.htm

NHS Information Governance (DH, 2007).
Available at
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616

Mental Capacity Act: 2005 Code of Practice (DCA, 2007)
Available at www.justice.gov.uk/guidance/mca-code-of-practice.htm

MAPPA (Multi Agency Public Protection Arrangements) guidance (2007)
Available at www.probation.homeoffice.gov.uk/output/page30.asp

Information Sharing: Guidance for practitioners and managers (HMG, 2008) and case examples, training materials and further information about powers/ legislation.
Available at www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00807-2008

Information Sharing: ICO guidance for organisations on Data Protection Act and other legislation including good practice notes, codes of practice and technical guidance notes.
Available at www.ico.gov.uk/Home/for_organisations/data_protection_guide.aspx

Information sharing: ICO Information sharing pocket.
Available at www.teachernet.gov.uk/publications. Search using the ref: DCSF-00808-2008

Information sharing: ICO Information Sharing Golden Rules. The Seven Golden Rules for information sharing is an extract from HM Government 'Information sharing: Guidance for practitioners and managers', DCSF 2008

Confidentiality and Disclosure of Health Information Toolkit (BMA, 2008)
Available at www.bma.org.uk/ap.nsf/Content/ConfToolKit08

MARAC (Multi-Agency Risk Assessment Conference) toolkits
Available at www.caada.org.uk/index.html

Guidance for children's services

Guidance on the Children Act 2004 (HMG, 2004)
Available at www.ecm.gov.uk/strategy/guidance

Sharing Personal and Sensitive Personal Information on Children and Young People at Risk of Offending: A Practical Guide (Youth Justice Board, 2005)
Available at www.yjb.gov.uk/publications

Child Health Promotion Programme (DH, 2006)
Available at www.dh.gov.uk/en/Publicationsandstatistics/Publications/DH_083645

Working Together to Safeguard Children and What to do if you are worried a child is being abused (HMG, 2006)
Available at www.ecm.gov.uk/safeguarding

0-18 years: guidance for all doctors (GMC, 2007)
Available at www.gmc-uk.org/guidance/ethical_guidance/children_guidance/index.asp

When to share information: Best practice guidance for everyone working in the youth justice system (2008)
Available at www.dh.gov.uk/en/Publicationsandstatistics/Publications/

Information Sharing – Advice for practitioners providing safeguarding advice to children, young people, parents and carers (2015)

Guidance for working with vulnerable adults

No secrets: guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse
Available at www.dh.gov.uk/en/Publicationsandstatistics/Publications/

23. Links to other information

Reaching Out: Think Family, analysis and themes from the Families at Risk Review (Cabinet Office, 2006) and Think Family: Improving the life changes of families at risk (Cabinet Office, 2008)
www.cabinetoffice.gov.uk/social_exclusion_task_force/families_at_risk.aspx

Local Safeguarding Children Boards information available at www.ecm.gov.uk/lscb

Every Child Matters (TSO, 2003)
Available at www.everychildmatters.gov.uk/aims/background/

Children's Centres – information available at www.surestart.gov.uk/surestartservices/settings/surestartchildrenscentres/

Youth Inclusion and Support Panels – information available at www.yjb.gov.uk/en-gb/yjs/Prevention/YISP/

Single Assessment Process – information available at www.dh.gov.uk/en/SocialCare/Chargingandassessment/SingleAssessmentProcess

Common Assessment Framework – information available at www.ecm.gov.uk/caf

ContactPoint – information available at www.ecm.gov.uk/ContactPoint

CWDC Share! (2007-08) – available from the Children's Workforce Development Council at www.cwdcouncil.org.uk/cwdc-share

Our Health, Our Care, Our Say (DH, 2006)
Available at www.dh.gov.uk/en/Healthcare/Ourhealthourcareoursay/index.htm

24. Links to legislative documents

Links to legislation referenced in this document are given below:

The Data Protection Act 1998. Information available at www.ico.gov.uk/what_we_cover/data_protection.aspx

Education and Inspections Act 2005. Information available at www.dcsf.gov.uk/publications/educationandinspectionsact/

Mental Capacity Act 2005. Information available at www.justice.gov.uk/guidance/mental-capacity.htm

National Health Service Act 2006. Information available at www.dh.gov.uk/en/Publicationsandstatistics/Legislation/Actsandbills/DH_064103

Safeguarding Vulnerable Groups Act 2006. Information available at www.opsi.gov.uk/ACTS/acts2006/ukpga_20060047_en_1

25. Links to documents related to bulk or pre-agreed information sharing

Data Protection and Sharing – Guidance for Emergency Planners and Responders (HMG, 2007). Available at www.ukresilience.gov.uk/response/recovery_guidance/generic_issues/data_protection.aspx

Data handling procedures across government. Information available at www.cabinetoffice.gov.uk/csia

Data Sharing Review Report (Richard Thomas and Mark Walport, 2008) Available at www.justice.gov.uk/docs/data-sharing-review.pdf

26. Links to council policies and procedures

The council's Information Governance Policy gives clear direction to staff on the legal requirements and best practice standards for managing council information.

The following council policies support the overall Information Governance Policy:

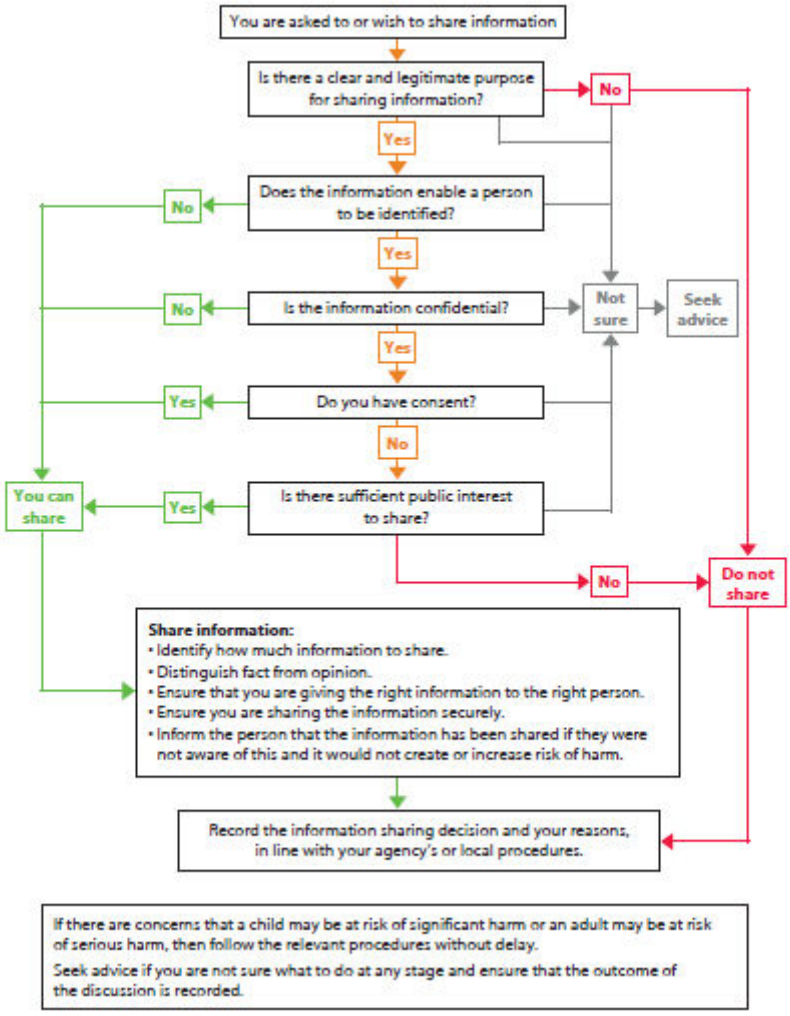
- Information Security Policy
- Records Management Policy
- Information Handling and Protective Marking Policy
- Data Protection and Privacy Policy
- Information Security - Mobile Working Policy
- Information Security Incident Reporting Policy
- Removable Media and Devices Policy
- Password Policy
- Email and Internet Usage Policy
- IT Hardware and Media Disposal Policy.

All of these policies can be downloaded from the IS&T forms, policies and procedures page.

Further information

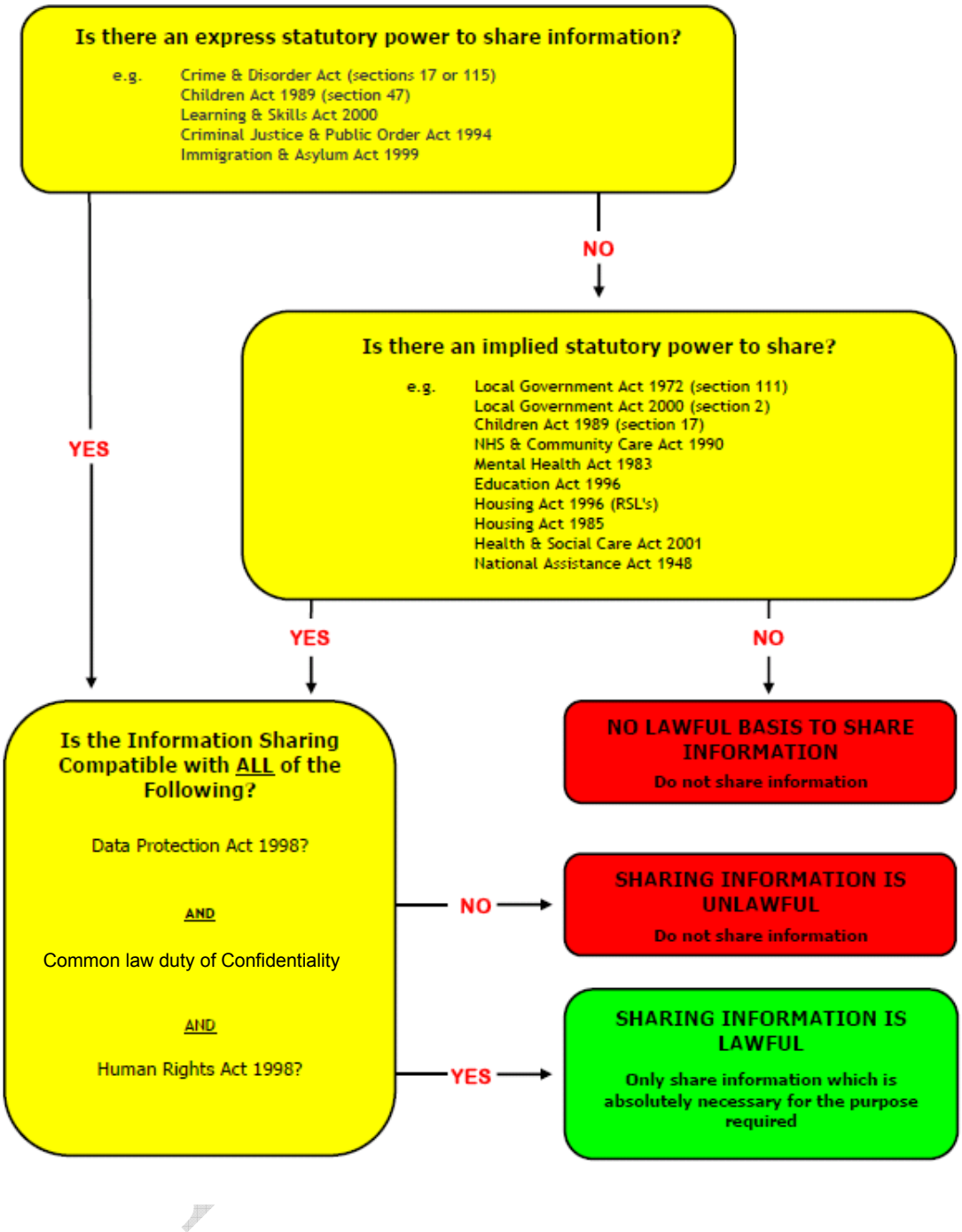
For further information on this issue, contact the council's Information & Records Manager on 01753 875070.

Annex 1: Flow chart of key questions for information sharing

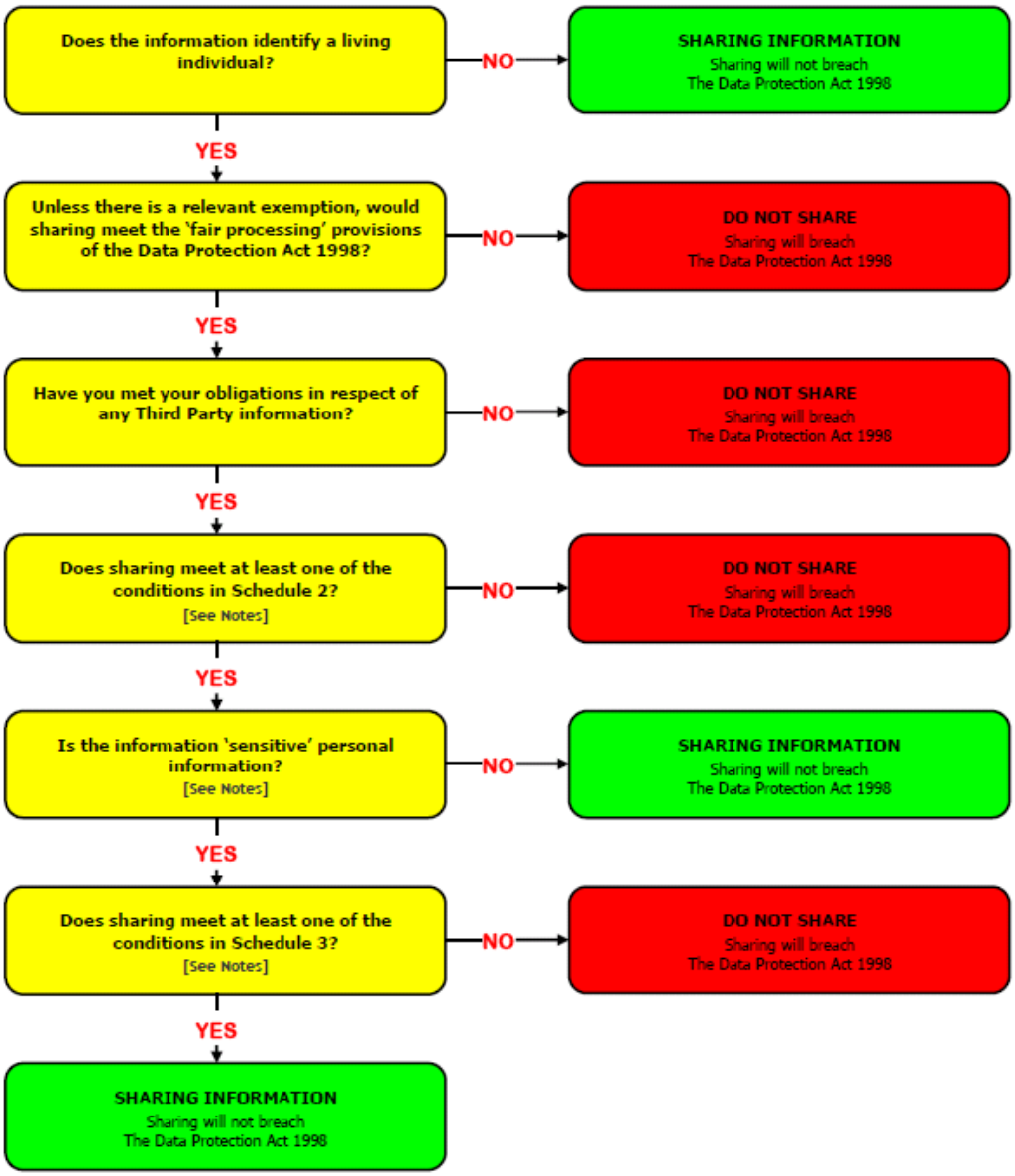


If after following the steps in this diagram, you have any doubts about the whether the proposed information sharing is lawful, you should seek advice from your line manager/your Designated Officer or the person with responsibility for data protection within your organisation.

Annex 2: Is information sharing lawful?



Annex 3: Is information sharing compatible with the DPA



Annex 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:

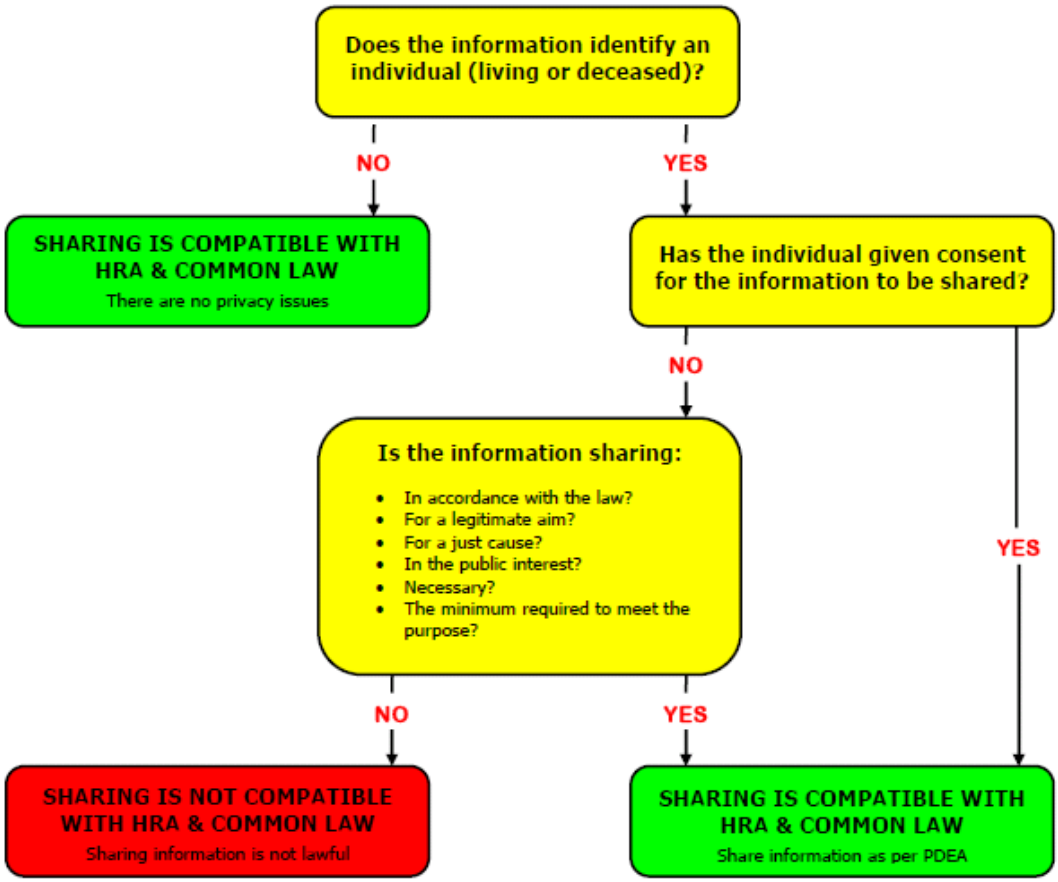
1. Racial or ethnic origin.
2. Political opinions / affiliations.
3. Religious beliefs or other beliefs of a similar nature.
4. Trade union membership.
5. Physical or mental health or condition.
6. Sexual orientation or activity.
7. Whether they have carried out or been accused of committing any offence.
8. Details of court proceedings for any offence committed or alleged to have been committed.
9. 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.

Annex 5: Is sharing compatible with HRA and 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.

Annex 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.

Annex 7: Specimen information sharing consent form

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	

Annex 8: Safe haven procedures for the secure handling of personal information

Safe Haven procedures in the context of this Protocol/Agreement cover:

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

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, texts & 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.

Annex 9: 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

Annex 10: Specimen disclosure request / record of disclosure

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.

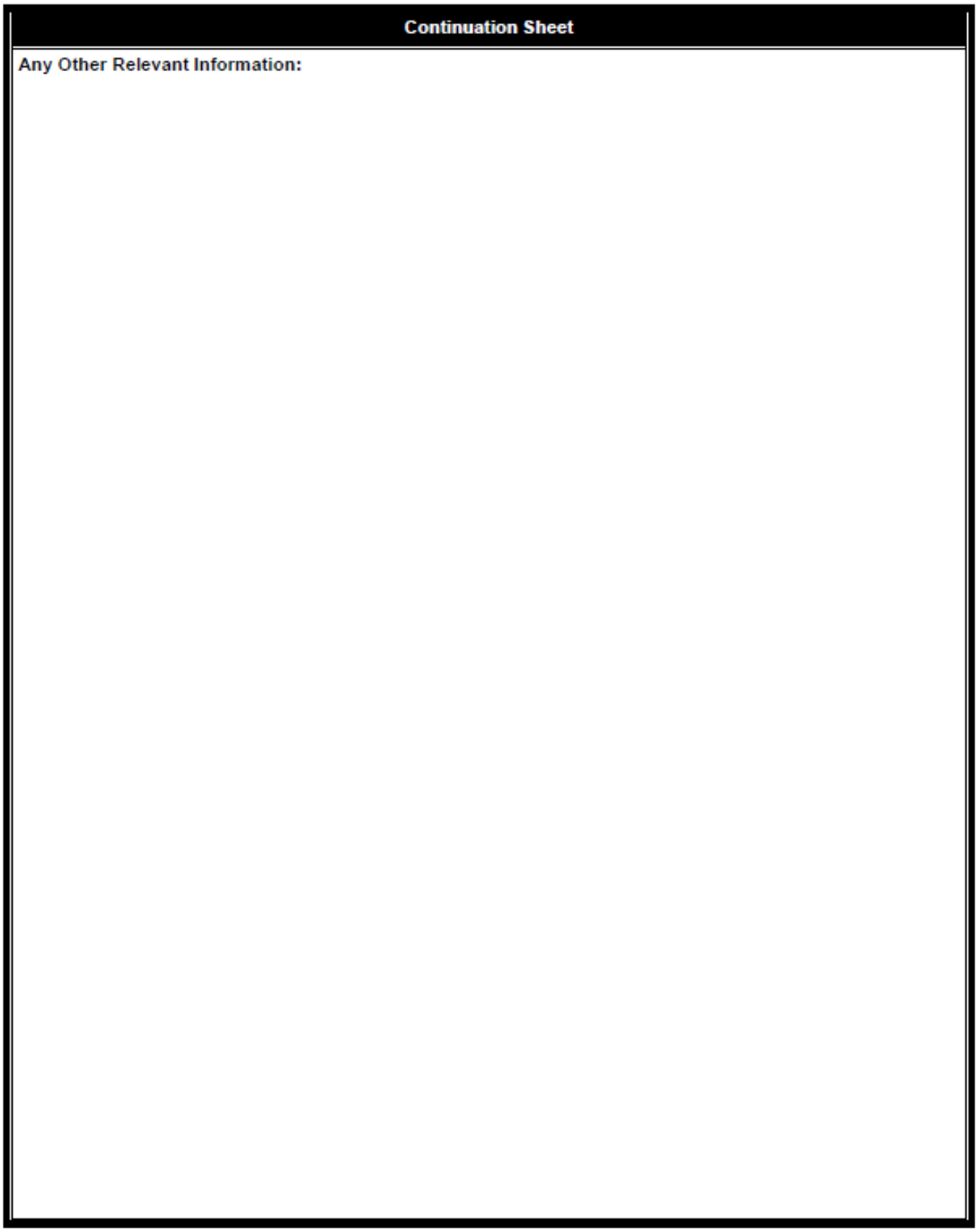
Request Received By			
Request Ref.		Disclosure Ref.	
Person		Post	
Receipt via		Date Received	

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.



Annex 11: Specimen Community Information Agreement

Community Information Agreement [Name of partnership/programme]

Document control

Author	
Contributors	
Version	
Date of production	
Review date	
Responsibility for review	
Primary circulation list	
Sign off	

Document history

Date	Version	Comments

Community Information Agreement

Contents

Community Information Agreement

1. Introduction

This agreement is made under [name of the over-arching information sharing protocol that applies. *For example: The Slough Wellbeing Board Overarching Information Sharing Protocol (OISP)]* between:

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

Note: The organisations signing up to this agreement must also be signatories to the overarching information sharing protocols detailed above.

2. Purpose of this agreement

This document is Tier Two level Community Information Agreement.

As such it is not a legally binding document.

It aims to provide the basis for an agreement between the agencies and other organisations engaged in *[insert the name and function of the partnership]* to facilitate and govern the efficient, effective and secure sharing of good quality information.

It sets out:

(a) The principles underpinning information sharing
(b) The general purposes for information sharing
(c) The responsibilities and commitments of partners to this agreement
(d) The arrangements for monitoring and review

This agreement complies with the information sharing principles defined in *[Slough Wellbeing Board's Overarching Information Protocol].*

It aligns with all other agreements to which agencies may already be signatories and does not in any way supersede those existing agreements.

This document is not intended to be definitive or exhaustive, it is recognised that as policy develops and implementation arrangements mature, this agreement will need to be reviewed and amended in light of new information sharing requirements to ensure that it is 'fit for purpose'.

As such this agreement aims to provide a set of guiding principles for information sharing within the context of *[provide the name of the programme, policy area or function for which the partnership has been formed]* to which partners can sign up, its purpose is not to be specific.

It is a key principle of Slough Wellbeing Board's Protocol that this agreement should be underpinned by a series of purpose specific data sharing agreements

that detail the specific data/information sharing requirements between partner organisations and agencies.

3. Policy context

[Enter statement that explains the policy area within which the partnership activities sit and what it aims to achieve through a multi-agency approach]

In order for the development of the *[enter name of programme]* to be successful it is essential that all agencies and organisations engaged in its development and implementation are empowered and committed to share good quality and relevant information in a responsible and secure way.

4. Scope

This agreement covers the sharing of information between all agencies and organisations engaged in/or who are identified as holding relevant information for the purposes of developing, implementing, monitoring and evaluating *[name of programme].*

A list of signatories is at Appendix A. This list is not exhaustive and will be updated regularly as part of the agreement monitoring and review process as required.

Information may be *[state types of information to be shared e.g. anonymised, personal and/or sensitive or confidential]* in nature and may be shared where *[state the basis for sharing e.g. is a legal power to do so, where informed consent has been sought].*

The relevance of the scope of the agreement should be considered as part of the *[name of programme]* a regular monitoring and review process.

This is not intended to be an exhaustive list as policy changes or delivery approaches mature and other purposes may be identified and these will be incorporated into this agreement during the monitoring and review process.

5. Type of personal information that will be shared

[Provide details of the broad categories of personal information to be routinely shared under this 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 Classified as sensitive personal*
- *Sexual life information under the DPA*
- *Racial or ethnic origin'*

Note: A combination of categories of personal information may apply under this agreement.

6. 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 this agreement*
- *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 this agreement*
- *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.*

7. Purposes for sharing information

Under the terms of this agreement information may be shared for any purpose that supports the development of the *[name of programme]* in *[place]* and that has been agreed within a specific information sharing agreement.

In general information sharing will be required to support the development and operation of *[name the programme/function]*.

This may include the following:*[List the different functions for which information will be require]*

8. Consent *[delete where consent is not to be used]*

Explicit consent will be sought from data subjects in accordance with individual partner agency policies and procedures where it has been identified as a necessary condition for the processing of the information as set out in the Data Protection Act 1998.

Where consent is required it is the responsibility of partner agencies to seek consent from their clients to share information for the purposes identified.

Where consent is refused or withdrawn by the data subject that information will not be used unless there is a risk of harm to the individual or others.

It should be made clear to the data subject/s the circumstances under which information will be shared with other agencies without their consent and the implications to them of not being able to share their information. The responsibility for ensuring this lies with the partner agency.

9. Lawful basis for the sharing of personal information

It is essential that all information shared under the terms of this agreement is done so in compliance with the following key legislation:

(a) The Data Protection Act 1998
(b) The Human Rights Act
(c) Common Law Duty of Confidentiality

In addition each agency / organisation signed up to this agreement will have their own legal framework that governs their functions and that sets out the circumstances under which personal and sensitive information may be shared.

The relevant legislation is as follows: *[Insert list of legislation]*

It is the responsibility of the individual agency/organisation to ensure that their data sharing transactions undertaken are done so legally and fairly and that they comply with their own legal powers and the legislation detailed above.

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

10. Key principles

In signing up to this agreement the signatories agree and commit to the following principles:

- This agreement aims to align with individual partner agency statutory, legal and common law duties.
- This agreement is to be entered into alongside any existing protocols, procedures, policies and guidance to which the partner already adheres and does not supersede them.
- This agreement will be underpinned by Tier 3 purpose specific information sharing agreements that will govern data sharing transactions between partners.
- Information will only be used for the purposes stated in this agreement, and as detailed in individual purpose specific information sharing agreements.
- Partner agencies comply with the requirements of the Data Protection Act 1998 and in particular the eight data protection principles

- Partner agencies support, endorse and promote the accurate, timely, secure and confidential sharing of information for the purposes stated in this agreement.
- Where it is agreed that it is necessary to share personal information it will be shared only on a 'need to know' basis and this will be detailed in the purpose specific information sharing agreement. All other information will be statistical and aggregated.
- Personal and sensitive Information will only be shared under this agreement where there is a statutory power to do so and the conditions for processing as determined in the Data Protection Act 1998 can be met.
- Agencies agree to ensure that data sharing takes place in accordance with their legal, statutory and common law duties and that responsibility for ensuring that they have adequate notifications, privacy notices, policies, procedures and guidance to do so remains with them.
- All information will be supplied in line with the relevant standards for information quality and security.

11. Supporting policies

[*List any supporting polices or procedures that signatories also have to follow in their partner organisation or agency here*].

12. Restrictions on the use of shared personal information

[List any specific additional restrictions that signatories to this agreement have on the use of personal information here].

13. Breaches of confidentiality

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

14. Complaints

Complaints about this disclosure of information under this agreements, or breaches of this agreement, will be dealt with under the complaints procedure of the partner organisation concerned.

15. Further framework documents

The signatories to this agreement will be responsible for developing and issuing purpose specific information sharing arrangement guidance and training to staff to ensure compliance with this agreement.

16. Governance, monitoring and review

The review, monitoring and amendment of this agreement will be undertaken by *[state who will be responsible].*

Formal review will be undertaken [annually] unless legislation or policy changes dictate otherwise.

New parties to this agreement may be included at any time, the formal arrangements for which will managed by *[state who will be responsible]* and agreed by *[state who will endorse the decision].*

All amendments to the agreement will be reported to and signed off *[insert who will be responsible for endorsing changes to this agreement].*

All will reviews of this agreement will have regard to:

(a) Changes in the relevant law and statutory or other government or national guidance;
(b) Service-user and staff opinions, concerns and complaints;
(c) Failures in compliance and disagreements between partner organisations;
(d) Any other relevant information.

17. Effective date

This agreement is effective from an agreed common implementation date of [insert date] and will be subject to a common review period [*insert period*] from the implementation date.

18. Termination of this agreement by an organisation

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

19. Conclusion

This agreement proposes a consistent approach to the sharing of information between partner agencies for the purposes of developing and implementing the *[name of programme].* All partners need to be able to balance the conflicting demands between the need to share information with other agencies and the requirement to maintain confidentiality. These conflicting demands are acknowledged by this agreement which provides a basis for partners to be confident that where information is shared it will be done in a consistent, responsible and secure way for the purpose of *[state the programme/partnership aims].*

20. Signatories to the agreement

Authorised signatories from each organisation listed in the table at appendix A accept this agreement.

Appendix A: Signatories to the *[Insert title*] Community Information Agreement

Organisation	Post/position	Name	Signature	Date

Appendix 12: Specimen Purpose Specific Information Agreement

Purpose Specific Information Agreement [Name of partnership/programme]

Document control

Author	
Contributors	
Version	
Date of production	
Review date	
Responsibility for review	
Primary circulation list	
Sign off	

Document history

Date	Version	Comments

Purpose Specific Information Agreement

Contents

Purpose Specific Information Agreement

1. Introduction

This agreement is made under [name of the over-arching information sharing protocol or community information agreement that applies. *For example: The Slough Wellbeing Board Over-Arching Information Sharing Protocol (OISP)]* between:

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

2. Purpose of this agreement

This document is Tier Three level Purpose Specific Information Sharing Agreement. As such it is not a legally binding document.

It aims to provide the basis for an agreement between the agencies and other organisations engaged in *[insert the name and function of the partnership]* to facilitate and govern the efficient, effective and secure sharing of good quality information.

It sets out:

(a) What information is to be shared
(b) What it is being shared (for what purpose)
(c) Who it is being shared with (between organisations and agencies)
(d) When it is being shared (the times and frequency etc)
(e) How is it being shared (format)

This agreement complies with the information sharing principles defined in *[Slough Wellbeing Board's Overarching Information Protocol].*

It aligns with all other agreements to which agencies may already be signatories and does not in any way supersede those existing agreements.

This document is not intended to be definitive or exhaustive, it is recognised that as policy develops and implementation arrangements mature, this agreement will need to be reviewed and amended in light of new information sharing requirements to ensure that it is 'fit for purpose'. As such this agreement aims to provide a set of guiding principles for information sharing within the context of *[provide the name of the programme, policy area or function for which the partnership has been formed]* to which partners can sign up, its purpose is not to be specific.

3. Policy context

[Enter statement that explains the policy area within which the partnership activities sit and what it aims to achieve through a multi-agency approach]

In order for the development of the *[enter name of programme]* to be successful it is essential that all agencies and organisations engaged in its development and

implementation are empowered and committed to share good quality and relevant information in a responsible and secure way.

4. Scope

This agreement covers the sharing of information between all agencies and organisations engaged in/or who are identified as holding relevant information for the purposes of developing, implementing, monitoring and evaluating *[name of programme].*

A list of signatories is at Appendix A. This list is not exhaustive and will be updated regularly as part of the agreement monitoring and review process as required.

Information may be *[state types of information to be shared e.g. anonymised, personal and/or sensitive or confidential]* in nature and may be shared where *[state the basis for sharing e.g. is a legal power to do so, where informed consent has been sought].*

The relevance of the scope of the agreement should be considered as part of the *[name of programme]* a regular monitoring and review process. This is not intended to be an exhaustive list as policy changes or delivery approaches mature and other purposes may be identified and these will be incorporated into this agreement during the monitoring and review process.

5. Who will share information?

Under this agreement, the following partners are required to share information under the [*list the legislation*].

[*List the organisations*]

Under this agreement, the following organisations may also be required to share information under the [*name relevant information/ legislation]*. These include

[List the organisations]

The following organisations may also be to share information under this agreement for [*specify the purpose/ name relevant information/ legislation].*

[List the organisations]

6. Type of personal information that will be shared

[*Provide details of the specific categories of personal information to be shared under this agreement and the state frequency.*

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 Classified as sensitive personal*
- *Sexual life information under the DPA*
- *Racial or ethnic origin'*

Note: A combination of categories of personal information may apply under this agreement.

Additional information may also be shared in order to maximise the ability of the [*insert name of partnership*] to deliver against its requirements.

7. How personal information will be shared

[Include a 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 this agreement*
- *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 this agreement*
- *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.*

Signatories to this agreement are responsible for ensuring that any data they supply is current, accurate and suitable for the purpose.

All data should be shared and stored in accordance with the relevant legislation.

Any information shared should only be kept as long as it is necessary and then destroyed.

8. Purposes for sharing information

Under the terms of this agreement information may be shared for any purpose that supports the development of the *[name of programme]* in *[place]* and that has been agreed within a specific information sharing agreement.

In general information sharing will be required to support the development and operation of *[name the programme/function]*.

This may include the following: *[List the different functions for which information will be required].*

9. Consent

Explicit consent will be sought from data subjects in accordance with individual partner agency policies and procedures where it has been identified as a necessary condition for the processing of the information as set out in the Data Protection Act 1998.

Where consent is required it is the responsibility of partner agencies to seek consent from their clients to share information for the purposes identified.

Where consent is refused or withdrawn by the data subject that information will not be used unless there is a risk of harm to the individual or others.

It should be made clear to the data subject/s the circumstances under which information will be shared with other agencies without their consent and the implications to them of not being able to share their information.

The responsibility for ensuring this lies with the partner agency.

10. Lawful basis for the sharing of personal information

It is essential that all information shared under the terms of this agreement is done so in compliance with the following key legislation:

(a) The Data Protection Act 1998
(b) The Human Rights Act
(c) Common Law Duty of Confidentiality

In addition each of the signatories to this agreement will have their own legal framework that governs their functions and sets out the circumstances under which personal and sensitive information may be shared.

The relevant legislation is as follows:

[*Insert list of legislation*]

It is the responsibility of each signatory to ensure that their data sharing transactions are done so legally and fairly and that they comply with their own legal powers and the legislation detailed above.

[Note: Whilst more than one piece of legislation may support the general information sharing framework, the purpose of this agreement is to clearly define specific, local information sharing initiatives. In view of this, the statutory powers to

share information under this agreement should ideally be confined to one 'key' piece of legislation.]

11. Roles and responsibilities of signatories

In signing up to this agreement, the signatories at appendices A and B to this agreement will undertake the following roles, responsibilities and actions in order to achieve agreement sign off' by *[state who will endorse the agreement]* and ensure that this agreement is maintained appropriately:

- Provide training to staff in the use of this agreement.
- Take steps to comply with the Data Protection Act, the Human Rights Act and the Caldicott Principles.
- Ensure that their organisational and security measures comply with ISO 27001, or equivalent internal standards, to protect the lawful use of information shared under this agreement.
- Ensure that all appropriate staff who have access to shared information have the necessary level of CRB clearance in accordance with relevant legislation.
- Only use the information for the purpose for which it has been shared.
- Use all reasonable actions to ensure that information provided under this agreement is, and remains, accurate.
- Record improvements in information sharing between each other, for example where information was not readily available before but where professionals now feel able to share.
- Ensure that senior managers provide advice and support in implementing this agreement and any operational arrangements, particularly when resolving disagreements within or between other partner organisations.
- Help ensure that service-users are made aware that this agreement governs the use of their personal information and provide copies on request.

12. Nominated representatives

Each signatory to this agreement shall have a lead nominated representative for the purpose of this agreement, who will ensure there are Designated Officers who will make and receive data-sharing requests and who will support further review of this agreement.

Nominated representatives will meet at least every [*specify when*], or as necessary, to discuss the working of this agreement.

A list of nominated representatives to this agreement can be found at appendix B. This list is not exhaustive and will be updated regularly as part of the agreement monitoring and review process as required.

Any disputes or disagreements between parties shall be resolved by discussion between the nominated representatives and/or between the heads of each organisation where appropriate.

13. Data controller responsibilities

Data controllers will make appropriate notification to the Information Commissioner as defined by the Data Protection Act 1998 and the Information Commissioner.

14. Agents and sub-contractors

Each signatory to this agreement will ensure that its agents and sub-contractors comply with the provisions of this agreement.

15. Arrangements for data sharing at multi-agency meetings [*delete where unnecessary]*

Meetings, such as [*insert name*], which regularly require partners to share information will be categorised according to the government protective marking[1] scheme and appropriate security procedures put in place accordingly.

All parties to this agreement understand that in keeping with government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the [insert relevant legislation], it is likely that there will be individuals present at certain meetings who are not representing an organisation which is a signatory to this agreement.

The first time any individual attends a meeting covered by this agreement, they should be required to sign a Confidentiality Agreement form.

[1] *'Protective marking' is the method by which the originator of an asset (that is all material assets, i.e. papers, drawings, images, disks and all forms of electronic data records), indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within the guidance and outside the originator's own department or force and its ultimate method of disposal.*

The ACPO guide to Protective Marking details this scheme and the security measures which need to be put in place to comply with it.

The levels of restriction are:

- *No protective marking*
- *Restricted*
- *Confidential*
- *Secret*
- *Top Secret*

The meeting organiser should clearly designate the meeting, using this scheme, prior to any information being shared and ensure that all partners are aware of the data handling and sharing requirements relevant to the designation.

Responsibility for ensuring that this takes place and for retaining a signed copy of this Confidentially Agreement form rests with the Chair of these meetings.

16. The process for data sharing outside meetings

If information is to be shared outside of the [*insert name of partnerships*] meeting structure, a brief Information Sharing Statement will be drawn up setting out the procedures that should be followed.

17. Key principles

In signing up to this agreement the signatories agree and commit to the following principles:

- This agreement aims to align with individual partner agency statutory, legal and common law duties.
- This agreement is to be entered into alongside any existing protocols, procedures, policies and guidance to which the partner already adheres and does not supersede them.
- Information will only be used for the purposes stated in this agreement.
- Partner agencies comply with the requirements of the Data Protection Act 1998 and in particular the eight data protection principles.
- Partner agencies support, endorse and promote the accurate, timely, secure and confidential sharing of information for the purposes stated in this agreement.
- Where it is agreed that it is necessary to share personal information it will be shared only on a 'need to know' basis. All other information will be statistical and aggregated.
- Personal and sensitive information will only be shared under this agreement where there is a statutory power to do so and the conditions for processing as determined in the Data Protection Act 1998 can be met.
- Agencies agree to ensure that data sharing takes place in accordance with their legal, statutory and common law duties and that responsibility for ensuring that they have adequate notifications, privacy notices, policies, procedures and guidance to do so remains with them.
- All information will be supplied in line with the relevant standards for information quality and security.

18. Supporting policies

[*List any supporting polices or procedures that signatories also have to follow in their partner organisation or agency here*].

19. Restrictions on the use of shared personal information

[List any specific additional restrictions that signatories to this agreement have on the use of personal information here].

20. Breaches of confidentiality

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

21. Complaints

All complaints about the disclosure of information under this agreement will be dealt with under the complaints procedure of the partner organisation concerned.

If two or more partner organisations receive a complaint about the same matter, they should investigate and respond to the complaint jointly.

If a partner receiving a complaint believes another partner may be responsible, wholly or partly, for the matters complained of, it should notify the other organisation and the organisations should investigate and respond to the complaint jointly.

22. Non-compliance and partner disagreement

In the event of a suspected failure within a partner organisation to comply with this agreement, the partner organisations will ensure that an adequate investigation is carried out and recorded.

If the partner finds there has been a failure it will ensure that:

- Necessary remedial action is taken promptly;
- Service-users affected by the failure are notified of it, the likely consequences, and any remedial action;
- Partner organisations affected by the failure are notified of it, the likely consequences, and any remedial action.

If one partner believes another has failed to comply with this agreement it should notify the other partner in writing giving full details.

The other partners will then investigate the alleged failure.

If they find there was a failure, they will take the steps set out above.

If they find there was no failure they will notify the first partner in writing giving their reasons.

Partners will make every effort to resolve disagreements between them about personal information use and sharing.

Nominated representatives will ensure they are notified at an early stage of any suspected or alleged failures in compliance or partner disagreements relating to their partner Organisation.

23. Governance, monitoring and review

The review, monitoring and amendment of this agreement will be undertaken by *[state who will be responsible].*

All formal reviews will be undertaken [*state when*] unless legislation or policy changes dictate otherwise.

All reviews of this review will have regard to:

- Changes in the relevant law and statutory or other government or national guidance;
- Service-user and staff opinions, concerns and complaints;
- Failures in compliance and disagreements between partners;
- Any other relevant information.

New signatories to this agreement can be included at any time, the formal arrangements for which will be managed by *[state who will be responsible]* and agreed by *[state who will endorse the decision].*

All amendments to this agreement will be reported to and signed off by *[insert who will be responsible for endorsing changes to this agreement].*

24. Effective date

This agreement is effective from an agreed common implementation date of [*insert date*] and will be subject to a common review period [*insert period*] from the implementation date.

25. Termination of this agreement by an organisation

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

26. Links to other Purpose Specific Information Agreements

Title	Effective From	Effective to	Lead Agency	Contact Details

27. Conclusion

This agreement proposes a consistent approach to the sharing of information between partner agencies for the purposes of developing and implementing the *[name of programme].*

All signatories to this agreement need to be able to balance the conflicting demands between the need to share information with other agencies and the requirement to maintain confidentiality.

These conflicting demands are acknowledged by this agreement which provides a basis for partners to be confident that where information is shared it will be done in a consistent, responsible and secure way for the purpose of *[state the programme/partnership aims]*.

28. Signatories to this agreement

Authorised signatories from each organisation listed in the table at appendix A accept this agreement:

Appendix A: Signatories to the *[Insert title*] Purpose Specific Information Agreement

Organisation	Post/position	Name	Signature	Date

Appendix B: List of Partnership Organisations, Signatory Persons and Nominated Representatives

Partnership member	Signatory person and position	Nominated representative	Contact details (include telephone number and email address)