Appendix B

Slough Wellbeing Board

Overarching Information Sharing Protocol

Guidance
July 2015

Document Control

Document details		
Document name	Slough Wellbeing Board's Overarching Information Sharing Protocol Guidance	
Document version number	*3.0*	
Document status	*Live*	
Author	*Amanda Renn, Policy Officer, Policy and Communications team*	
Lead Officer	*Tracy Luck, Assistant Director, Strategy and Engagement*	
Approved by		
Scheduled review date		
Version History		
Version	**Change/Reasons for Change**	**Date**
1	*Initial draft prepared*	*March 2015*
2	*Minor changes needed to paragraph 5 to reflect Legal Service's advice*	*April 2015*
3	*(a) Information concerning the requirements of the Freedom of Information Act 2000 added at the request of TVP* *(b) Information about the Police Act 1996, the Crime and Disorder Act 1998, Caldicott principles and legal powers to share added* *(c) Minor changes made to annex 11* *(d) Minor changes made to annex 12* *(e) Links to other sources of information removed (will be published separately on the council's website)* *(f) Glossary added at annex 13* *(g) Guidance shortened throughout*	*June 2015*
Approval history		
Version	**Approving body**	**Date**
2	*Slough Wellbeing Board*	*13 May 2015*
3	*Slough Wellbeing Board*	*15 July 2015*

Slough Wellbeing Board

Overarching Information Sharing Protocol

Guidance

Contents

Slough Wellbeing Board

Overarching Information Sharing Protocol Guidance

Please note this document has been prepared as a guide and there may well be a requirement to include further sections or make amendments to this document as necessary.

In all instances please refer to your Information Governance lead officer for further guidance and support.

1. Foreword

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 too.

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 also 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 guidance has been developed to help elected members, council employees and other organisations working in partnership with the Slough Wellbeing Board, meet their statutory requirements and the expectations of the people they serve.

Following this guidance will ensure compliance with the law when sharing personal information between Wellbeing Board members and other public, private or voluntary sector organisations that they work, or wish to work, in partnership with.

This guidance also applies to anyone working in a voluntary capacity within those organisations.

3. Scope

This guidance 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 Protocol.

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

4. Definitions

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.

5. Information sharing framework

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

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

- Slough Wellbeing Board's Overarching Information Sharing 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 framework (see below).

Tier 2 - Community Information Sharing Agreements (CISA)
- These agreements are high level agreements common to organisations and agencies delivering health, social and community services.
- They satisfy Tier Two level of the Slough Wellbeing Board's Information Sharing framework and focus on the collective **purposes** 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 Sharing Agreements (PSISA) (Tier 3) (see below), which set out at a detailed level, how personal information will be shared amongst organisations within the same information community.
- Community Information Agreements are usually signed by Service Directors or the equivalent functional leads.
- A specimen CISA is at **annex 11**.

Tier 3 - Purpose Specific Information Sharing Agreements (PSISA)
- These agreements are the lowest level of the Slough Wellbeing Board's Overarching Information Sharing framework.
- They are aimed at an organisation's "operational management/practitioner" level and define the relevant **procedures** 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.
- A specimen PSISA is at **annex 12**.

6. Conditions for sharing information

All of the signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol have agreed that they will:

- Adhere to and demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998 (DPA) and other associated privacy legislation.

- Adhere to/or demonstrate commitment to achieving the appropriate compliance with guidance published by the Information Commissioner's Code of Practise's Fair Processing and Best Practise Standards and any other guidance published by the Information Commissioner's Office.
- Develop and agree individual information sharing agreements that detail the specific data sharing arrangements that exist between partner organisations and agencies.
- Promote staff awareness of the requirements of information sharing and support the production of appropriate guidelines where required.
- 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 intended.
- Where information sharing agreements between partner organisations and agencies already exist prior to members having signed up to the Slough Wellbeing Board's Overarching Information Sharing Protocol, these agreements will remain valid. However, these agreements 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.
- A flow chart of key questions partner organisations need to ask when looking to develop an individual information agreement under the Wellbeing Boards Protocol is at **annex 1**.
- Annex 5 also provides additional guidance on this issue.

7. The legal position in respect of information sharing

7.1 Legal framework

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

(a) The Data Protection Act 1998 (DPA)

- Data Protection legislation governs the standards for the processing of personal data including the collection, use and disclosure of such information. The legislation requires that Data Controllers meet certain obligations.
- It also gives individuals or 'Data Subjects' certain rights with regard to their own personal data.
- The main standard for processing personal data is compliance with the eight data protection principles summarised as follows:
  - All personal data will be obtained and processed fairy and lawfully.
  - Personal data will be held only for the purposes specified.
  - Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data is held.
  - Personal data is accurate and where necessary, kept up to date.
  - Personal data will be held for no longer than is necessary.

- Personal data will be processed in accordance with the Rights of the Data Subject.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing for personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to countries outside the European Economic Area (EEA) except in limited circumstances.

- The first principle states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Schedule 2 condition and in the case of 'sensitive personal data', at least one Schedule 3 condition is also met.
- The type of information being disclosed may constitute 'sensitive personal data' which means that at least one of both Schedule 2 and Schedule 3 conditions must be satisfied.
- Even in the event that the prevention and detection of crime exemption (Section 29 Data Protection Act) is being relied upon, or other power such as S.115 Crime and Disorder Act, Schedules 2 and 3 conditions must still be satisfied.
- **Annex 3** explains these conditions in more detail.
- Although the aforementioned conditions are likely to apply to any or all of the variable circumstances, it is likely that for the purposes of most individual information sharing agreements one of the additional conditions specified in secondary legislation, for example: S.I No 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000 and (Daft) The Data Protection (Processing of Sensitive Personal Data) Order 2006, may also apply.

Data Protection (Processing of Sensitive Personal Data) Order 2000

- The Order lists additional circumstances in which sensitive personal data may be processed. For example, it covers processing for purposes of the prevention or detection of any unlawful act, where seeking the consent of the data subject would prejudice those purposes.
- It also covers processing required to discharge functions involving the provision of services such as confidential counselling and advice where the subject's consent has not been obtained. In each of the examples above, processing would have to be 'in the substantial public interest'. This could mean for example, that processing is necessary to protect public safety or to protect vulnerable people.

Data Protection (Processing of Sensitive Personal Data) Order 2006

- The Order specifies that information about a criminal conviction or caution may be processed for the purpose of administering an account relating to the payment card used in the commissioning of one of the listed offences relating to indecent images of children

(b) The Human Rights Act 1998 (HRA) (Article 8)

- The UK Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention of Human Rights (ECHR).
- The Act requires all domestic law to be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

- Article 8 of the Act states that: *'Everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law'.*
- It is likely that this exchange of information will be for the purposes of one of the following legitimate aims:
  - In the interests of nation security
  - Public Safety
  - Economic well-being of the country
  - The prevention crime and disorder
  - The protection of health or morals
  - The protection of the rights or freedoms of others
- 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.

(c) The Freedom of Information Act 2000 (FOIA)

- Information held by or behalf of a public authority may be disclosed to a party requesting it except where statutory exemption applies. For example, personal data is normally exempt under the Act (but may be disclosable under the DPA); as is information provided under a duty of confidence.

(d) The Common Law Duty of Confidence

- 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.
- This duty falls within common law as opposed to statutory law and derives from cases considered by the courts.
- There are generally three categories of exception to the duty of confidence:
  - Where these is a legal compulsion to disclose
  - Where there is an overriding duty to the public
  - Where the individual to whom the information relates consented
- It 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.
- Partner organisations should consider which conditions are the most relevant ones for the purposes of their individual information sharing agreements.

- The guidance from the Information Commissioner states that because such decisions to disclose 'in the public interest' involve the exercise of judgment, it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions.
- Partner organisations should document within their individual agreements how this duty will be maintained, e.g. need to know.
- Other legislation/requirements may also be relevant when sharing specific types of information:
- **Annex 5** explains this in more detail.

(e) Caldicott principles

- Where health data is concerned; when sharing information with others, due regard must be given to the following Caldicott principles:
  - Justify the purpose before sharing information.
  - Only use patient identifiable data when absolutely necessary.
  - Use the minimum that is required, do not share more data than is necessary, i.e. do not send the whole patient record when only the request relates to a recent event.
  - Access to the data should be on a strict need to know basis.
  - Staff must be aware of their responsibilities in complying with organisational policies relating to confidentiality.
  - Understand the law, if uncertain; staff should speak to their line manager or the appropriate Caldicott Guardian.
  - The duty to share information can be as important as the duty to protect patient information.
  - Ensure that wherever possible the NHS number is present and person identifiable data has been removed.
- Partner organisations must ensure that all these conditions are met before sending any data.
- Where Health Data is concerned Health staff and others working in partnership with them, should be aware of the concept of Safe Haven. Safe Havens will:
  - Provide a secure location restricting access to only authorised staff and will be locked outside normal hours.
  - Be staffed by those individuals with authority to access confidential information and who are under contractual and statutory obligations to maintain confidentiality.
- Ensure that no confidential information will be released to parties outside the Trust unless it is deemed appropriate. Health Staff should make reference to the Caldicott Principles listed above and seek advice from their Caldicott Guardian where uncertain.
- **Annex 8** provides further information on this issue.

(f) Legal Government Act 2000

- The main power specific to local authorities is section 2 Local Government Act 2000 – the power of 'well-being'.
- This enables local authorities to do 'anything' to promote social, economic or social well-being in their area provided the act is not specifically forbidden by general powers available to local authorities.

- In addition, authorities are granted statutory powers relating to specific activities and these should be referred to as appropriate in relevant information sharing agreements or other statutes (including the DPA) and that in carrying out the Act it gives regard to its own community strategy. For example, all councils are taking measures, including data sharing, to reduce crime in their area in order to promote well-being.
- In addition s.111 Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place.
- The above are granted statutory powers relating to specific activities and these should be referred to as appropriate in relevant information sharing agreements.

(g) The Police Act 1996

- The Police Act 1996 gives a Constable certain powers.
- Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment whenever passed or made.
- These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.
- In addition, the Code of Practice on the Management of Police Information 2005 defines the policing purpose as:-
  - Protecting life and property
  - Preserving order
  - Preventing the commission of offences
  - Bringing offenders to justice
  - And duty or responsibility arising from common or statute law
- The policing purpose set out in the Code does not replace or supersede any existing duty or power defined by statute or common law.
- In addition this does not define every policing activity and does not mean that there is no legal basis for performing such activities. For example, roads policing, public order, counterterrorism or protection of children or other vulnerable groups while not referred to explicitly are none the less legitimate policing functions.

(h) The Crime and Disorder Act 1998

- Section 115 of the Crime and Disorder Act 1998 confers power on any 'relevant authority' (which are the police, local authority, health authority and probation service or to any other person acting on behalf of such authority) to exchange that information which is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder.
- The parties to this exchange agreement are relevant authorities for the purposes of this legislation.
- Section 17 Crime and Disorder Act 1998 requires that all local authorities consider crime and disorder reduction while exercising their duties.

- Section 5 and 6 of the Crime and Disorder Act also imposes a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area**.**

7.2 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.

8. 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 possesses 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.

9. 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.

10. 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 CISA or PSISA 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.

11. Consent

11.1 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 (DPA) 1998

- In the case of non-sensitive personal information, an alternative Schedule 2 condition is met; or
- In the case of sensitive personal information, an alternative Schedule 2 **AND** an alternative Schedule 3 condition are met: and
- 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
- 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 (HRA) (Article 8)

- The information has no connection with and cannot impact on the private life of the individual; or
- It is in accordance with the law; and
- It is necessary in a democratic society; and
- It is for a legitimate aim; and
- It is proportionate.

Common Law Duty of Confidentiality

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

11.2 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

11.3 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**.

11.4 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.

11.5 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.

11.6 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 CISA or PSISA. If the purpose of the specific partnership significantly changes it may be necessary to seek fresh consent.

11.7 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.

11.8 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.

12. 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 the disclosure of and receipt of information shared under any individual information sharing agreement are created under it. This is in order to:

  (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.

(d) A specimen Disclosure Request / Record of Disclosure form can be found at **annex 10**.

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

(f) It is best practice to adopt and use information sharing notice and attendance sheet on such occasions.

(g) A specimen can be found at **annex 9**.

13. Security and retention of information

All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are required to put in place appropriate policies and procedures covering the security, storage, retention and destruction of personal information.

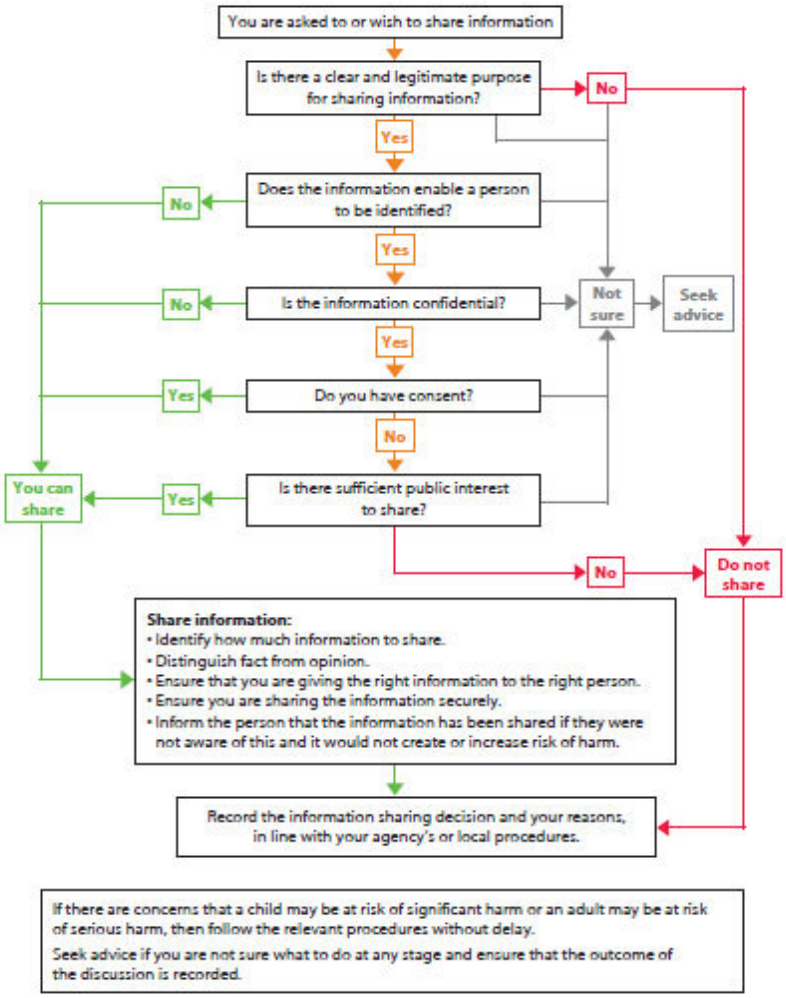
For the purposes of information sharing under Slough Wellbeing Board's Overarching Information Sharing Protocol, each partner organisation will ensure that the transfer or transmission of personal information is via secure means.

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

14. Notification requirements of partner organisations

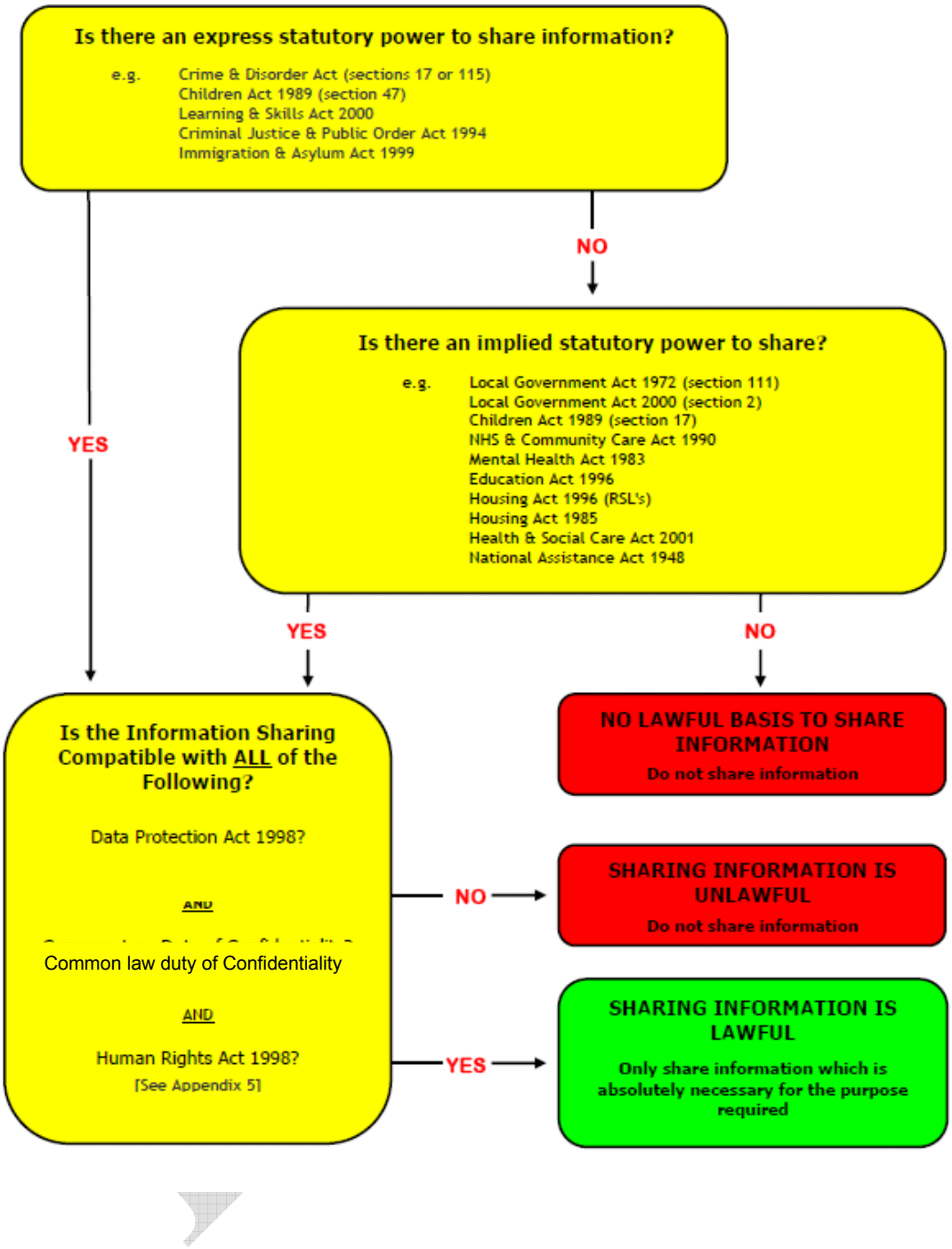
- All signatories to Slough Wellbeing Board's Overarching Information Sharing Protocol are responsible for ensuring that their DPA notifications to the Information Commissioner's Office cover the information sharing arrangements established under the Board's Overarching Information Sharing Protocol and any individual agreements created under it.

Annex 1: Flow chart of key questions for information sharing

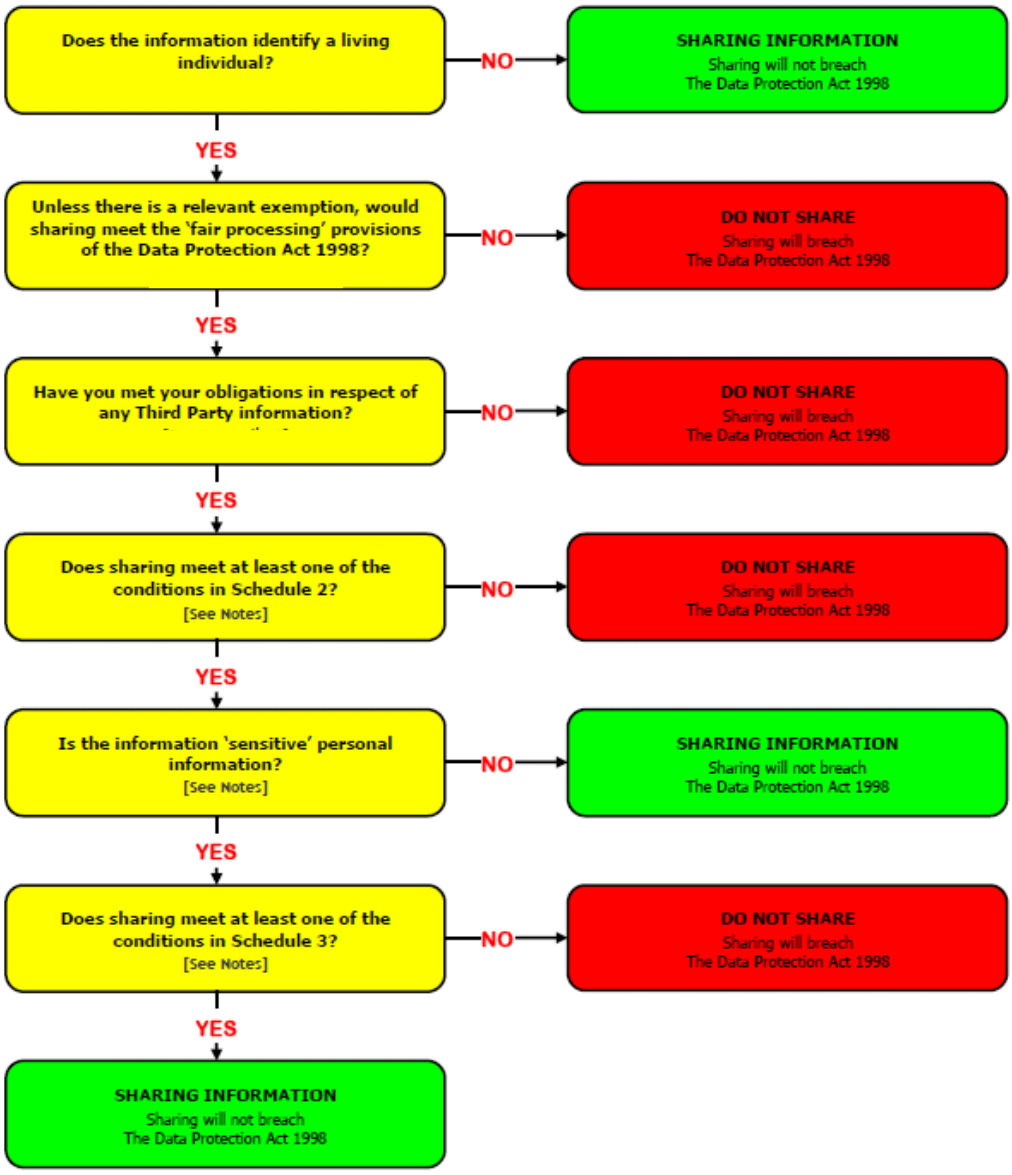


If after following the steps in this diagram, you have any doubts about the whether the proposed information sharing is lawful, you should seek advice from your line manager/your Designated Officer or the person with responsibility for data protection within your organisation.

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 person's 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.
10. Processed in circumstances ordered by the Secretary of State, to include matters deemed to be in the substantial public interest, for the prevention of fraud and malpractice, and necessary for the exercise of any functions conferred on a constable.[1]

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.

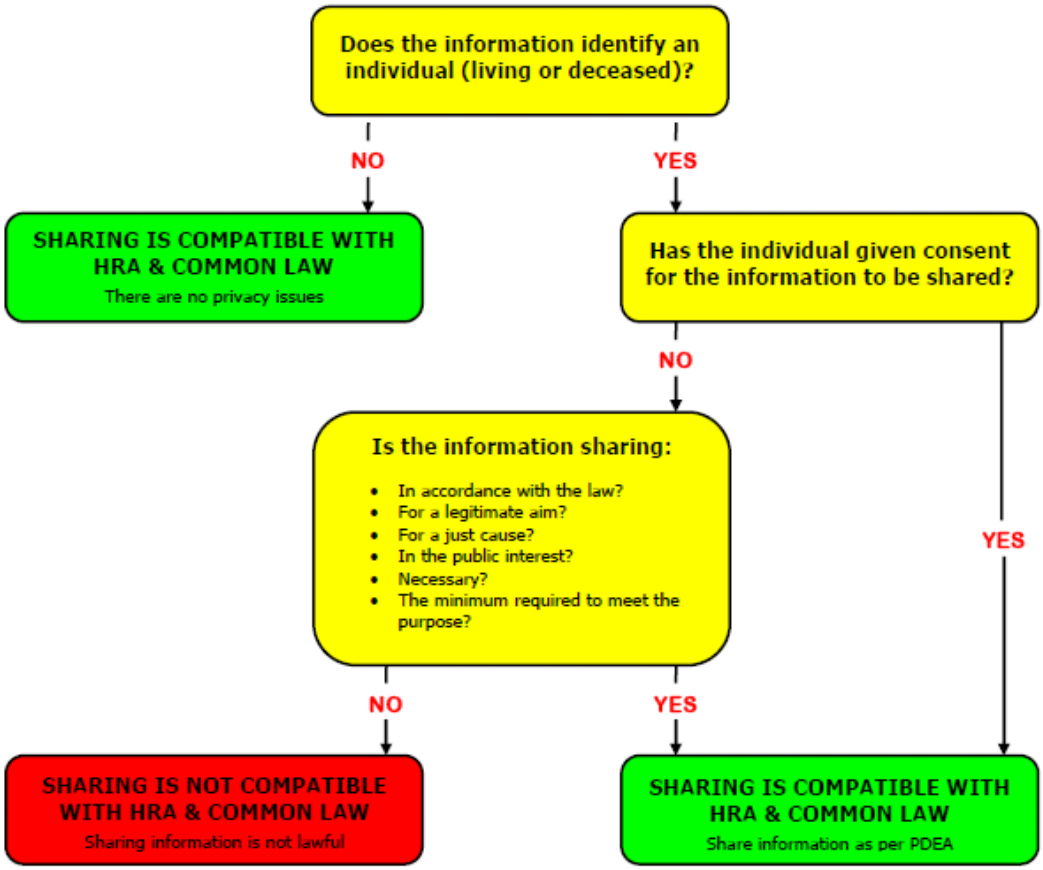
[1] *As required under The DP (Processing of Sensitive Personal Data) Order 2000*

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 individual's rights;
7. Secure; and
8. Not transferred to countries without adequate protection.

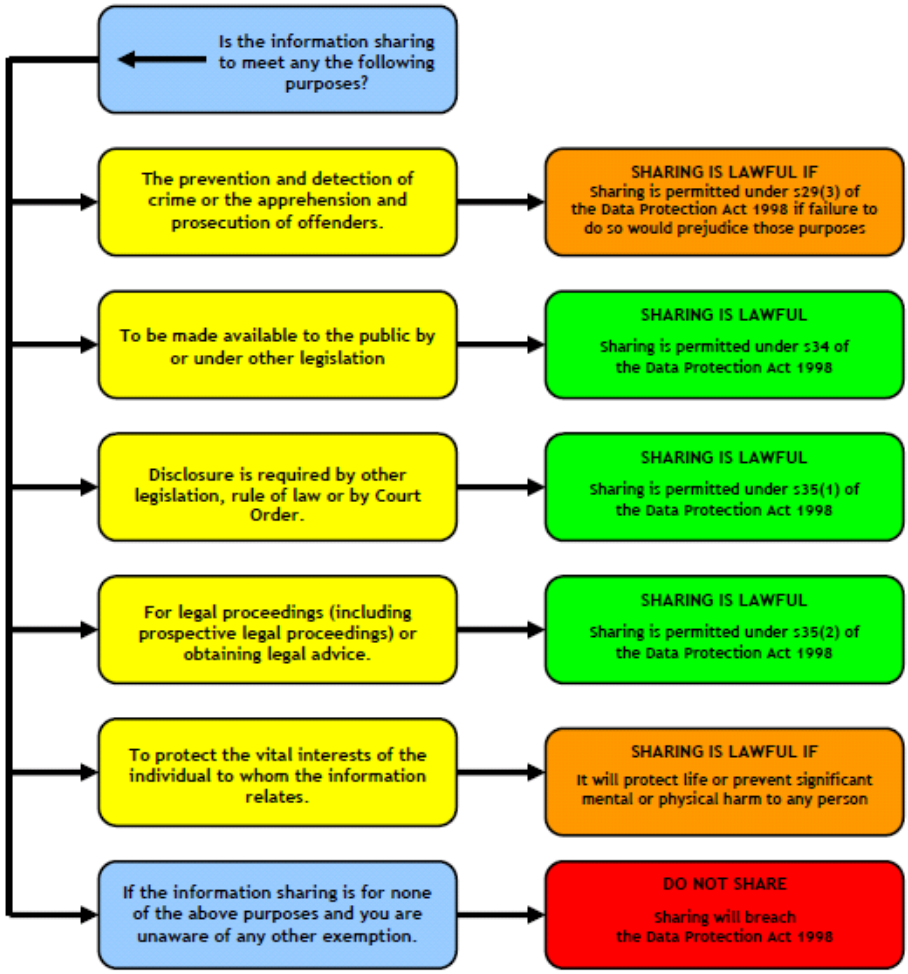
Annex 5: Is sharing compatible with HRA and Common Law?



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.

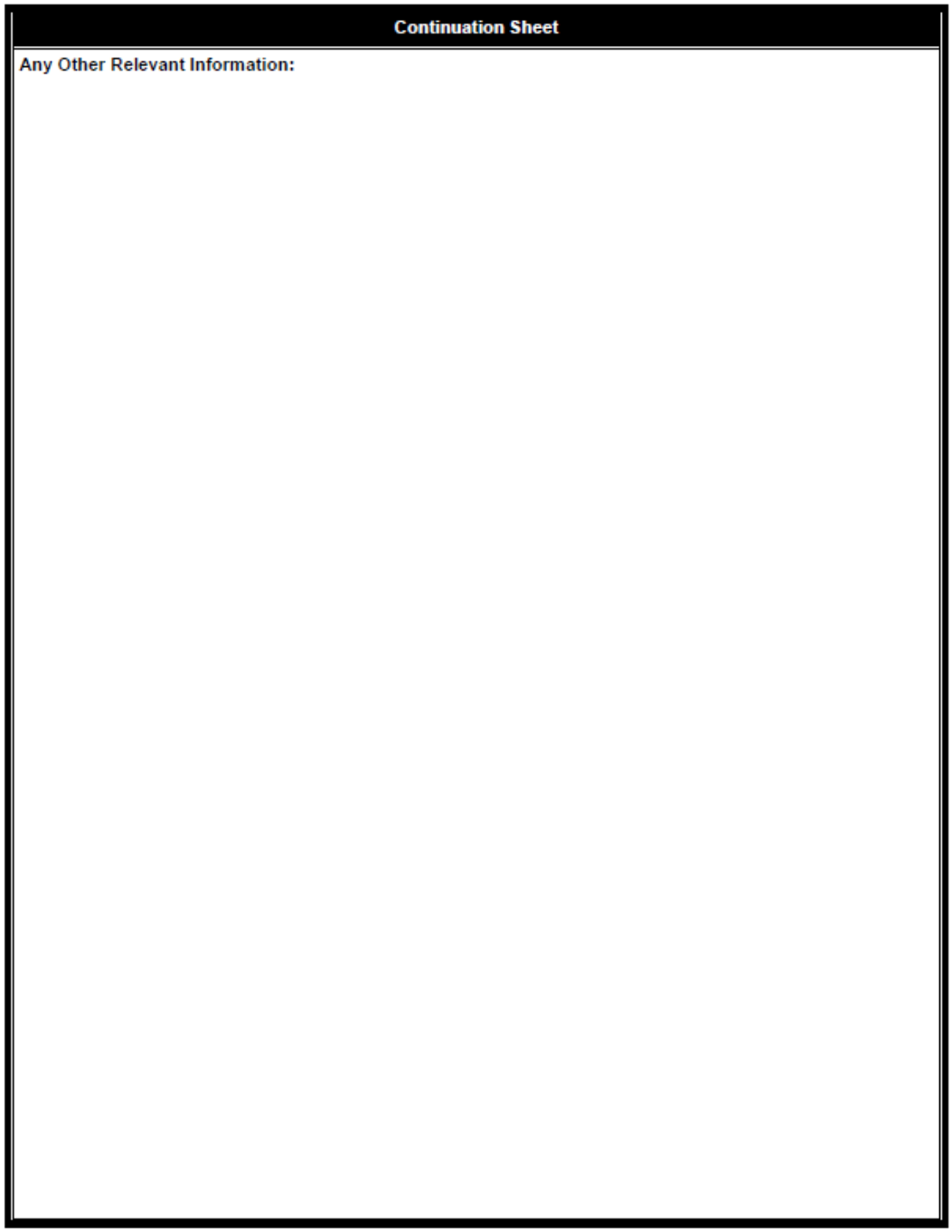
Request Received By			
Request Ref.		Disclosure Ref.	
Person		Post	
Receipt via		Date Received	

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 Sharing Agreement

Community Information Sharing 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 Sharing Agreement

Contents

[insert details]

Community Information Agreement

1. Forward

This agreement is the agreement between the partner organisations and agencies detailed in annex 1 to govern the sharing of information.

It provides the framework for the secure and confident sharing of information between partner organisations in order to satisfy the requirements of the law and guidance regulating working practises and provides guidance to operational staff.

2. Purpose of agreement

This agreement relates to […….]

The purpose of this agreement is for […….]

The purpose of this agreement is primarily so that […….].

It sets out:

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

3. Slough Wellbeing Board's Overarching Information Sharing Protocol

Slough Wellbeing Board's Overarching Information Sharing Protocol provides a framework for the secure and confidential sharing of information between partnership organisations and agencies in order to satisfy the requirements of the law and central guidance regulating to working practise and provides operational guidelines for staff.

The purpose of Slough Wellbeing Board's Protocol is to facilitate and govern the sharing of information to enable partner's organisations and agencies to meet their responsibilities to protect, support and care for individuals within the Slough community.

Slough Wellbeing Board's Protocol comprises the common principles which will be adopted whenever the partner organisations and agencies listed in annex A have to share information and covers the sharing of information for any of the following purposes:

- Improving and supporting the health and social care for people
- Protecting people and communities
- Prevention and detection of crime
- Investigating complaints
- Developing interagency strategies and co-ordinating the provisions of care.

Partner organisations and agencies which are party to the Slough Wellbeing Board's Protocol are required to comply with both the statutory and organisational policies when using information shared between one or more of the parties. Therefore, there must either be informed consent given from the data subject that their personal data will be shared with a 3rd party organisation (as we are working in partnership), or alternatively, if informed or explicit consent cannot be obtained there must be reliance upon another statutory requirement to do so.

The Slough Wellbeing Board's Protocol will be supplemented by individual information sharing agreements and guidance for staff, specific to particular applications/situations, which will set out the detailed arrangements relevant to that particular application.

All individual agreements will be fully compliant and consistent with the Wellbeing Board's Overarching Protocol.

It is acknowledged that this agreement is in accordance with fair processing under the Data Protection Act 1998 (DPA), but as a local agreement all information will be processed in accordance with the Slough Wellbeing Board's Overarching Information Sharing Protocol.

4. 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.]

5. Agreed use of information

The information will only be used for the purpose stated within this agreement (as specified in section 2) but will permit the information to be used for the purposes of additional service planning and provision

The agreement allows the frequent exchange of the specified information and the processes will be reviewed on a regular basis by the organisations concerned.

6. How personal information will be requested

[Insert a statement explaining the method(s) that will be used to ensure:

- *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*
- *The availability of requested personal information.*
- *The 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. Methodology/process (example wording)

Information will be provided electronically from (…) to (…) who will disseminate it appropriately and securely.

This information will be sent in (word/excel) format as an attachment over secure mail or sent by *(insert alternative methods).*

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 (DPA)
(b) The Human Rights Act 1998 (Article 8) (HRA)
(c) Freedom of Information Act 2000 (FOIA)
(d) Common Law Duty of Confidence

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.

10. Data Protection Act – subject access request

Under DPA legislation individuals have the right of access to any personally identifiable information held about them, This right may be defined in certain limited circumstances and will be defined in local; organisations and agencies policies an in statute(e.g. DPA).

Where a party to this agreement receives a request for information and compliance with that request would involve disclosing information relating to another individual who can be identified from that information, they should not comply with that request unless:

- The other individual has consented to the disclosure of the information to the person making the request; or
- Compliance with the request can be justified on the grounds of a greater public interest overriding the individual's right to confidentiality; or
- The information is capable of anonymisation so that the individual cannot be identified.

Where a party to this agreement seeks to rely on an exemption to the disclosure of personal information under the DPA, it needs to consider in light of other relevant information, whether failure to disclose would be likely to adversely affect the treatment or services given to the service user.

The decision made must take into account all the relevant circumstances of the case in the balance and if necessary further legal advice should be taken. Deliberations should be fully documented so that the reasons behind the decision are clear.

Consideration should be given to all aspects of the FOIA with regards to ownership of the data, for example if the holding organisation has a request for data under the FOIA, then proper process should be followed to ensure that both the holding organisation and the owning organisation are compliant with the act.

Where a party of this agreement receives a request for information and compliance with that request would involve disclosing information relating to another individual

who can be identified from that information, they should seek guidance from the organisation's Information Governance lead officer.

11. 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].

12. Breaches of confidentiality

[Include a statement explaining how breaches of confidentiality will be monitored and dealt with].

13. Complaints

[Include a statement explaining how complaints will be monitored and dealt with by the partner organisation concerned].

14. 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 complaint.
(c) Failures in compliance and disagreements between partner organisations.
(d) Any other relevant information.

15. 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.

16. Termination of this agreement by an organisation

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

17. Supporting policies

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

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

Organisation	Post/position	Name	Signature	Date

Annex 12: Specimen Purpose Specific Information Sharing Agreement

Purpose Specific Information Sharing 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

[Insert details]

Purpose Specific Information Sharing Agreement

1. Forward

This agreement is the agreement between the partner organisations and agencies detailed in annex 1 to govern the sharing of information.

It provides the framework for the secure and confident sharing of information between partner organisations in order to satisfy the requirements of the law and guidance regulating working practises and provides guidance to operational staff.

2. Purpose of this agreement

This agreement relates to […….]

The purpose of this agreement is for [……]

The purpose of this agreement is primarily so that […….].

It sets out the **procedures** that need to be followed, including:

(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)

3. Slough Wellbeing Board's Overarching Information Sharing Protocol

Slough Wellbeing Board's Overarching Information Sharing Protocol provides a framework for the secure and confidential sharing of information between partnership organisations and agencies in order to satisfy the requirements of the law and central guidance regulating to working practise and provides operational guidelines for staff.

The purpose of Slough Wellbeing Board's Protocol is to facilitate and govern the sharing of information to enable partner's organisations and agencies to meet their responsibilities to protect, support and care for individuals within the Slough community.

Slough Wellbeing Board's Protocol comprises the common principles which will be adopted whenever the partner organisations and agencies listed in annex A have to share information and covers the sharing of information for any of the following purposes:

- Improving and supporting the health and social care for people
- Protecting people and communities
- Prevention and detection of crime
- Investigating complaints
- Developing interagency strategies and co-ordinating the provisions of care.

Partner organisations and agencies which are party to the Slough Wellbeing Board's Protocol are required to comply with both the statutory and organisational policies when using information shared between one or more of the parties. Therefore, there must either be informed consent given from the data subject that their personal data will be shared with a 3rd party organisation (as we are working in partnership), or alternatively, if informed or explicit consent cannot be obtained there must be reliance upon another statutory requirement to do so.

The Slough Wellbeing Board's Protocol will be supplemented by individual information sharing agreements and guidance for staff, specific to particular applications/situations, which will set out the detailed arrangements relevant to that particular application. All individual agreements will be fully compliant and consistent with the Wellbeing Board's Overarching Protocol.

It is acknowledged that this agreement is in accordance with fair processing under the Data Protection Act 1998 (DPA), but as a local agreement all information will be processed in accordance with the Slough Wellbeing Board's Overarching Information Sharing Protocol.

4. 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.

5. 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].*

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.

6. 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]

7. 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.]

8. Agreed use of information

The information will only be used for the purpose stated within this agreement (as specified in section 2 and 4 above) but will permit the information to be used for the purposes of additional service planning and provision

The agreement allows the frequent exchange of the specified information and the processes will be reviewed on a regular basis by the organisations concerned.

9. How personal information will be requested

[Insert a statement explaining the method(s) that will be used to ensure:

- *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*
- *The availability of requested personal information.*

- *The 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.*

10. Methodology/process (example wording)

Information will be provided (specify) from (…) to (…) who will disseminate it appropriately and securely.

This information will be sent in (word/excel) format as an attachment over secure mail or sent by *(insert alternative methods).*

11. 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.

12. 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 (DPA)
b) The Human Rights Act 1998 (HRA)
c) The Freedom of Information Act 2000 (FOIA)
d) 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.

13. Data Protection Act – subject access request

Under DPA legislation individuals have the right of access to any personally identifiable information held about them, This right may be defined in certain limited circumstances and will be defined in local; organisations and agencies policies an in statute(e.g. DPA).

Where a party to this agreement receives a request for information and compliance with that request would involve disclosing information relating to another individual who can be identified from that information, they should not comply with that request unless:

- The other individual has consented to the disclosure of the information to the person making the request; or
- Compliance with the request can be justified on the grounds of a greater public interest overriding the individual's right to confidentiality; or
- The information is capable of anonymisation so that the individual cannot be identified.

Where a party to this agreement seeks to rely on an exemption to the disclosure of personal information under the DPA, it needs to consider in light of other relevant information, whether failure to disclose would be likely to adversely affect the treatment or services given to the service user.

The decision made must take into account all the relevant circumstances of the case in the balance and if necessary further legal advice should be taken. Deliberations should be fully documented so that the reasons behind the decision are clear.

Consideration should be given to all aspects of the FOIA with regards to ownership of the data, for example if the holding organisation has a request for data under the FOIA, then proper process should be followed to ensure that both the holding organisation and the owning organisation are compliant with the act.

Where a party of this agreement receives a request for information and compliance with that request would involve disclosing information relating to another individual who can be identified from that information, they should seek guidance from the organisation's Information Governance lead officer.

14. Roles and responsibilities of signatories

In signing up to this agreement the signatories at annex A agree to and commit to observe the following principles:

- Align this agreement with their individual organisation or agencies statutory, legal and common law duties.
- Only use information for the purposes stated in this agreement.
- Comply with the requirements of the Data Protection Act 1998 and in particular the eight data protection principles.
- 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.
- Only share personal and sensitive information where there is a statutory power to do so and where the conditions for processing as determined in the Data Protection Act 1998 can be met.
- Ensure that data sharing takes place in accordance with signatories 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.
- Supplied information in line with the relevant standards for information quality and security.

The signatories at annex A of this agreement also agree to 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 DAP, HRA, FOIA 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.

15. 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 annex 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.

16. 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.

17. Agents and sub-contractors

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

18. 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[2] scheme and appropriate security procedures put in place accordingly.

---

[2] *'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*

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.

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.

19. The process for data sharing outside meetings

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

20. 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].

21. 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.

- *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.

- 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.

22. Breaches of confidentiality

[Include a statement explaining how breaches of confidentiality will be monitored and dealt with].

23. Complaints

[Include a statement explaining how complaints will be monitored and dealt with by the partner organisation concerned].

24. 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.

25. 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.

26. Termination of this agreement by an organisation

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

27. Supporting policies

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

28. Links to other Community Information Sharing Agreements

[List relevant agreements here]

29. Links to other Purpose Specific Information Sharing Agreements

[List relevant agreements here]

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

Organisation	Post/position	Name	Signature	Date

Annex A continued: 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)

Annex 13 - Glossary

Aggregated – Collated information in a tabular format.

Anonymised data – Data where an Organisation does not have the means to identify an individual from the data they hold. If the Data Controller has information, which allows the Data Subject to be identified, regardless of whether or not they intend to identify the individual is immaterial – in the eyes of the Information Commissioner this is not anonymous data – see Pseudonimised data. The Data Controller must be able to justify why and how the data is no longer personal.
CCTV – Close circuit television.

Consent – The Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defined consent as '…any feely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' (3.1.5) data or Information –
a) Information being processed by means of equipment operating automatically; or
b) Information recorded with the intention it being processed by such equipment.
c) Recorded as part of a relevant filing system; or
d) Not in (a), (b) or (c), but forming part of an accessible record.
e) Recorded information help by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller – A person or a legal body such as a business or a public authority who jointly or alone determines the purposes for which personal data is processed.

Data Flows – The movement of information internally and externally, both within and between organisations.

Data Processing – Any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Processor – Operates on behalf of the Data Controller. Not staff.

Data Subject – An individual who is the subject of personal information.

Disclosure – The passing of information from the Data Controller to another organisation or individual.

Duty of Confidentiality – Everyone has a duty under the Common Law to safeguard personal information.

EEA – European Economic Area (EEA) – this consists of the fifteen EU members together with Iceland, Liechtenstein and Norway.

Fair Processing – To inform the Data Subject how the data is to be processed before processing occurs.

Information Agreement – The local Information Sharing Agreement based on the attached templates (see Annexes 11 and 12).

Informed consent – In order to comply with the Data Protection Act, to validate implied consent if necessary and to satisfy moral obligations, the sender must always strive to fully inform the subject wherever possible of the uses to which their information will be put, what disclosure could envisaged and what the consequences of the processing are. All parties must strive to be open and transparent.

Health Professional – The Data Protection Act 1998 defines a health professional as: a medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor and osteopaths. Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends to clinical psychologist, child psychotherapist and speech therapist, music therapist employed by health service body and scientist employed by such a body as head of department.

Health Record – Any information relating to health produced by a health professional.
HIV - Human Immunodeficiency Virus.

Need to know – To access and supply the minimum amount of information required for the defined purpose.

Personal Data – Means data relating to a living individual who can be identified from that data (including opinion and expression of intention).

Processing – Any operation performed on data. Main examples are collection, retention, use, disclosure and deletion.

Pseudonymised data – Where personal information has been 'de-identified' i.e. personal information which directly identifies an individual, e.g. name or date of birth and address used together, has been replaced by non-identifying, artificial data, e.g. NHS number or other code. Pseudonimised data is partially anonymised data and the identification of an individual can be re-established using other available data held by the Data Controller organisation. See also anonymised data.

Purpose – The use/reason for which information was originally collected for processing.

Recipient – Anyone who receives personal information for the purpose of specific inquires.

Relevant Filing System – Two levels of structure, (i) filing system structured by some criteria (ii) each file structured so that particular information is readily accessible.

Sensitive Personal Data – The DPA defines sensitive personal data as:
(a) the racial or ethnic origin of the data subject;
(b) his/her political opinions;

(c) his/her religious or other beliefs of a similar nature;
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992;
(e) his/her physical or mental health or condition;
(f) his/her sexual life;
(g) the commission or alleged commission by him/her of any offence; or
(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Subject Access – the individual's right to obtain a copy of information held about themselves.