Appendix A

Slough Wellbeing Board's Overarching Information Sharing Protocol

July 2015

Document Control

Document details	
Document name	Slough Wellbeing Board's Overarching Information Sharing Protocol
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*	*March 2015*
2	*(a) Minor changes needed to paragraph 5 of the Protocol to reflect Legal Service's advice; and* *(b) Guidance and templates brought into the main body of the Protocol as appendices (and original appendices and annexes renumbered accordingly).*	*April 2015* *April 2015*
3	*(a) Information concerning the requirements of the Freedom of Information Act 2000 added at the request of TVP* *(b) Strengthened Partner responsibilities section* *(c) Added Organisational responsibilities section* *(d) Added Individual responsibilities section* *(e) Protocol shortened throughout* *(f) Guidance section removed to create a separate standalone guide* *(g) Changes made to signatory panel at Annex A* *(h) Confidentiality statement added at Annex B*	*May 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

Contents

Appendices

Slough Wellbeing Board's Overarching Information Sharing Protocol

1. Introduction

This document is an Overarching Information Sharing Protocol (and for the purposes of this Protocol, the terms data and information are synonymous).

The aim of this document is to facilitate the sharing of information in accordance with the law between the public, private and voluntary sectors so that:

(a) Members of the public receive the services they need.
(b) Public sector services are delivered in line with government initiatives and public expectations.
(c) Services are planned, delivered and managed cost effectively and efficiently.

2. Background

Organisations that are 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 individuals 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 be unclear. This may lead to information not being available to those who have a genuine need to know, in order for them to carry out their work effectively.

This Protocol (and its accompanying best practice guide) has been developed to ensure that the Slough Wellbeing Board and other organisations and agencies working in partnership with it, comply with the law.

It sets out the rules that all people working for, or with partners organisations, must follow when using and sharing information.

This Overarching Information Sharing Protocol sets out the <u>principles</u> for information sharing between the partner organisation and agencies identified at annex A.

Under the terms of this Protocol, individual signatory organisations and agencies are expected to develop and agree individual information sharing agreements that deal with their specific needs in relation to information and data flows – particularly with regard to crime and disorder or the sharing of information about children.

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

It is not, however, intended that this Protocol will replace existing local organisational agreements or policies - but by formalising the role of the Slough Wellbeing Board through this Protocol, it provides a standardised approach to information sharing and

to do so confidentially whilst respecting an individual's rights of privacy concerning compliance with the relevant statutory obligations.

3. Scope

This Protocol applies to the organisations and agencies (listed in annex A), elected members and all of the employees of the council and said partner organisations and agencies, who are involved in partnership working arrangements under this Protocol.

It also applies to other public sector, private and voluntary organisations working in partnership with the signatories to this Protocol to deliver services.

This Protocol will be further extended to include other public sector, private and voluntary organisations and agencies working in partnership with the Slough Wellbeing Board to deliver services, where appropriate.

This Protocol applies to the following information:

- All personal information processed by the organisations and agencies (listed in annex A) including electronic systems (e.g. computer systems, CCTV, audio etc.) or in manual records.
- Anonymised (including aggregated) personal data. The considerations though less stringent, must take into account factors such as commercial and or business sensitive data and the effect of any data sets being applied.

The purposes for using and sharing information and the procedures that will be followed, will be defined in specific information sharing agreements.

These agreements will be individual to partner's organisations and agencies arrangements for sharing information and managing data flows.

4. Aims and objectives

This **aim** of this Protocol is to:

- Provide a robust framework for partner organisations and agencies that need to share personal data; and
- To establish and regulate working practises between partner organisations and agencies.

This Protocol also provides guidance to ensure the secure transfer of information and that information is shared for justifiable 'need to know' purposes.

The **objectives** of this Protocol are to:

- Guide partner organisations and agencies on how to share personal information lawfully.
- Identify the lawful basis for information sharing.
- Explain the security and confidentiality laws and principles of information sharing.

- Provide guidance on the legal requirements associated with information sharing.
- Increase awareness and understanding of the key issues involved.
- Emphasise the need to develop and agree individual agreements (where appropriate).
- Support processes and procedures that will monitor and review all data flows.
- Explain security requirements relating to the sharing of information.
- Encourage appropriate flows of data.
- Protect partner organisations and agencies from accusations of unlawful use of sensitive personal data.

5. Partners responsibilities

By becoming a signatory to this Protocol, partner organisations and agencies have agreed to:

- Apply and evidence that they have complied with Slough Wellbeing Board's best practise guide on information sharing, 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.
- Adhere to and demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998 (DPA) and other associated privacy legislation.
- Develop and agree local information sharing agreements that detail the data sharing arrangements for specific, individual information sharing initiatives between partner organisations (see Slough Wellbeing Board's best practise guide for example templates).
- Apply and evidence NHS Caldicott confidentiality standards where appropriate.
- Promote staff awareness of the major requirements for information sharing.
- Produce local guidelines (where required) for staff via their intranet sites and /or via other communications media.

6. General principles

This Protocol has been written to set out clear and consistent principles that satisfy the requirements of the law that all staff must follow when using and sharing personal information. The principles outlined in this Protocol are recommended good practice and/or legal requirements that should be adhered to by all partners' organisations and agencies.

This Protocol should be used in conjunction with local service level agreements, MOUs, contracts or any other formal agreements that exist between partner organisations and agencies.

This Protocol sets the core standards applicable to all partner organisations and agencies that should be used to inform the basis of all individual information agreements established to secure the flow of personal information.

The specific purposes and procedures that will be followed for using and sharing information will be defined in individual agreements and will be specific to the partner organisations and agencies sharing information.

7. Legal requirements

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

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

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

8. Data covered by this Protocol

Data covered by this Protocol refers to all personal identifiable information as defined in the DPA and as amended by the FOIA (Section 68).

8.1 Personal Information

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

The term is further defined in the DPA as:

- Data relating to a living individual who can be identified from the data, or
- Any other information which is in the possession of, or is likely to come into the possession of the Data Controller (i.e. person or organisation collecting or processing that information).
- Consideration should also be given to relevant case law that is defined as personal data such as the Durant ruling.

The DPA also defines certain classes of personal information as 'sensitive data' where additional conditions must be met for that information to be used and disclosed lawfully. An individual may consider certain information about them to be particularly 'sensitive' and may request data items to be kept especially confidential e.g. any use of pseudonym where their true identity needs to be withheld to protect them.

All medical data is deemed to be 'sensitive personal data' and is held under a duty of confidence.

8.2 Anonymised Data

Partner organisations and agencies must ensure anonymised data is not capable of being matched especially when combined with any additional information that could lead to the identity of individual, either directly or by summation.

Anonymised data about an individual can, in some circumstances, be shared without consent (subject to certain restrictions regarding health/social care records) and regard to secondary use principles.

9. Purpose for sharing information

- Each partner organisation and agency will operate lawfully in accordance with the DPA and its principles at all times.
- Information should only be shared for a specific lawful purpose, basis or where appropriate consent has been obtained.
- Staff should only have access to personal information on a justifiable need to know basis, in order for them to perform their duties in accordance with the services they are there to deliver.
- Having this Protocol (or any individual agreement developed to support it) does not give licence for unrestricted access to information another partner organisation and agency may hold: it simply lays the parameters for the safe and secure sharing of information for a justifiable 'need to know 'purpose.
- All staff should follow the standards that have been agreed within this Protocol and the processes and procedures that are included in any associated individual information sharing agreements developed in support of it.
- Every member of staff has an obligation to protect confidentiality and is responsible for ensuring that information that is only disclosed to those who have a right to see it.
- All staff should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information.
- Staff contracts should (where appropriate) contain a clause on confidentiality which all employees are bound by.
- Clinical/social care staff are also bound by their appropriate professional codes of conduct.

10. Restrictions on use of information shared

- Information must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant, associated information sharing agreement.
- It is a condition of access that it must not be used for any other purpose without the permission of the Data Controller who supplied the data, unless an exemption applies within the DPA or the information is required to be provided under the terms of the FOIA or any other statutory obligation.
- Additional statutory restrictions apply to the disclosure of certain information for example: Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection.
- Information about these will be included in the relevant organisational information sharing agreement.

11. Consent

- Consent is not the only means by which data can be disclosed. Under the DPA, in order to disclose personal information, at least one condition in Schedule 2 must be met. In order to disclose sensitive personal information at least one condition in both Schedules 2 and 3, must be met.
- Where a partner organisation or agency has a statutory obligation to disclose personal information, then the consent of the data subject is not required; the data subject should be informed that such an obligation exists. However the common law duties of confidence may still exist or prohibit this disclosure.

- If a partner organisation or agency decides not to disclose some or all of the personal information, the requesting authority must be informed. For example the partner organisation or agency may be relying on an exemption or on the inability to obtain consent from the data subject.
- Consent has to be signified by some indication on the part of the data subject to the data controller organisation. It is the provider organisation or agencies responsibility therefore to ensure that the necessary consent to share criteria has been satisfied as implied consent can often not be relied upon. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the Data Subject's consent must be clear and cover items such as the specific details of processing; the data to be processed and the purpose for processing.
- If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.
- Specific procedures will apply where the data subject is either under the age of 16, or where the data subject does not have the capacity to give informed consent. In these circumstances the relevant policy of the partner organisation and agency or agency should be referred to.
- Consideration should also be given to other case law, such as the Fraser Guidelines and the requirements of the Mental Capacity Act 2005.

12. Organisational responsibilities

- Each partner organisation and agency is responsible for ensuring that their organisational security measures protect the lawful use of information shared under this Protocol.
- Partner organisations and agencies will agree to all appropriate security measures necessary for the protection of the supplied information and will at all times handle the information accordingly.
- Partner organisations and agencies accept responsibility for independently or jointly auditing compliance with the individual information sharing agreements that they are involved within reasonable time-scales and where this is appropriate to do so.
- Each partner organisation and agency is responsible for ensuring that their employees, agents or contractors abide by the agreed rules and policies in relation to protection, security and use of confidential information.
- Any failure by an individual to follow these policies should be dealt with in accordance with that organisation's disciplinary procedures.
- Each partner organisation and agency should ensure that their contracts with external service providers abide by their rules and policies in relation to the protection and use of confidential information. The partner organisation and agency originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.
- Partner organisations and agencies should have well documented policies for the retention, weeding and secure waste destruction of information.
- Each partner organisation and agency is responsible for putting in place systems to record the disclosure and receipt of information shared under this Protocol and any individual agreement created under it. These systems should:
    - Create an audit trail to identify wrongful or excessive sharing of information.
    - Allow partner organisations and agencies 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.
  - 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.
  - Enable partner organisations and agencies to meet their obligations with respect to subject access requests which (unless an exemption applies) include informing the individual of the source of information and details of to whom it has been disclosed. In most instances, this will simply be a matter of recording the fact on the file / record. However, particular care must be taken to record instances where sensitive personal information is shared without consent. Partner organisations and agencies must ensure that any requests to disclose information in such circumstances and the disclosures that result in response to these requests are documented using a Disclosure Request / Record of Disclosure form.
- Each partner organisation and agency should ensure that any information sharing which occurs during multi-agency or partnership meetings is also recorded using an Information Sharing notice and Attendance sheet.
- Partner organisations and agencies should be committed to having procedures in place to ensure the quality of information i.e. that they consider having a Data Quality Strategy. A strategy will secure and ensure the maintenance of good quality standards and identify areas for improvement.
- Partner organisations and agencies must be aware that the Data Subject may withdraw consent to processing (i.e. Section 10 DPA) unless an available exemption applies. Where the partner organisation and agency relies on consent as the condition for processing, then withdrawal means that the condition for processing will no longer apply. Any such withdrawal of consent should be communicated to partner organisations and agencies and processing cease as soon as possible.
- Partner organisations and agencies are expected to have procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals must be provided with information about these procedures. *In the event of a complaint regarding the disclosure or use of personal information that has been supplied / obtained under this Protocol, or any individual agreements made under it, all organisations party to this Protocol or the individual agreement will provide co-operation and assistance in the investigation and resolution of the complaint.*
- The sixth principle of the DPA provides individuals the right to access information held about them, with limited exemptions. Partner organisations and agencies are therefore expected to ensure that only appropriate access to information is granted and to ensure that appropriate procedures are in place to ensure an individual's rights are met.
- Partner organisations and agencies must also ensure that their data protection Notifications to the Information Commissioner are appropriately maintained and reflect any information provided by an external agency.

13. Individual responsibilities

- Each individual working for an organisation or agency listed in annex A of this Protocol is personally responsible for the safekeeping of any information they

obtain, handle, use and disclose in relation to any individual agreements developed and agreed under this Protocol.

- Each individual should know how to obtain, use and share information they legitimately need to do their job.
- Each individual has an obligation to request proof of identity or takes steps validate the authorisation of another before disclosing any information.
- Each individual should uphold the general principles of confidentiality and follow the rules laid down in this Protocol and seek advice when necessary.
- Each individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal.
- Criminal proceedings might also be brought against that individual.

14. Access rights

- Under section 7 of the DPA, individuals have a right of access to personal information held about them, subject to any relevant exemptions which may apply. This means that any information provided by a partner organisation or agency under this Protocol (and any individual agreement created under it) may be disclosed to the individual without the need to obtain the provider's consent. However, the partner organisation or agency will be expected to consult with the provider if they have any concerns, and in particular if:

  (a) The provider has previously stated that the information supplied is subject to an exemption and therefore should not be disclosed to the individual.
  (b) The partner organisation or agency 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 and agencies have a joint (single) record on an individual, that individual may make their request for access to either partner organisation or agency. In such cases, the organisation receiving the request will be responsible for processing the request to the whole record and not just the part that they may have contributed, subject to the conditions detailed above.

15. Monitoring

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

  (a) A refusal by a partner organisation or agency to disclose information when requested.
  (b) Conditions being placed on disclosure.
  (c) Delays in responding to requests.

(d) Disclosure of information to members of staff who do not have a legitimate reason for access.
(e) Inappropriate or inadequate use of procedures e.g. insufficient information provided.
(f) The use of information for purposes other than those agreed.
(g) Inadequate security arrangements.
(h) Any actual or attempted security breach by an external party (e.g. hacking).
(i) Subject access requests.
(j) Any actions or omissions, which staff consider to be a breach of this Protocol, individual agreements or any relevant legislation.

16. Review of this Protocol

- This Protocol will be reviewed annually by the members of the Slough Wellbeing Board, unless new revised legislation or national guidance necessitates and earlier review.
- Any of the signatories to this Protocol can request an extraordinary review at any time should they consider it necessary.
- If during the course of this review it becomes evident that changes are required, all parties will be informed of the fact.
- All partner organisations and agencies will be expected to provide assistance in identifying and implementing any amendments that are required.

16.1 Review of any individual agreements made under this Protocol

- Any individual agreements made under this Protocol will specify a regular review period, typically an annual occurrence, but this may be shorter or longer depending on the nature of the partnership working taking place.
- In addition, any party to an individual agreement can request an extraordinary review at any time should they consider it necessary.
- Reasons to request an extraordinary review of an individual agreement may include significant changes in the nature of the partnership working or service delivery.
- If during the course of this review, it becomes evident that changes are required, all of the parties to the relevant agreement will be informed of the fact.
- All parties to the relevant agreement will also be expected to provide assistance in identifying and implementing any amendments that are required.

Annex A: Signatures and contact information

Agreement:

We the undersigned do hereby agree to implement the terms and conditions of this Protocol and confirm that we have read understood and agree to:

The Confidentiality Statement at Annex B

Slough Borough Council

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Thames Valley Police (TVP)

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Slough Council for Voluntary Services

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Clinical Commissioning Group Slough

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Head of Prevention and Protection, Royal Berkshire Fire and Rescue Service (RBFRS)

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Slough Healthwatch

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

NHS Commissioning Board

Name:	
Signature:	
Position:	
Contact Name:	
Telephone:	
Email:	

Annex B: Confidentiality statement

To enable the exchange of information to be carried out in accordance with the Data Protection Act 1998 (DPA), the Human Rights Act 1998 (HRA), the Freedom of Information Act 2000 (FOIA) and the Common Law Duty of Confidence, all parties are asked to agree to the following.

This information sharing activity contains confidential person (and where applicable patient) identifiable information. In order to comply with the law protecting confidentiality, the information can only be supplied subject to the following conditions:

(a) A senior member of staff in your organisation must take personal responsibility for maintaining confidentiality.
(b) The information is stored in a secure environment at all times.
(c) Once the task has been completed, and wherever possible (there may be a justifiable reason to retain data which is in the subjects best interest), the original information and all copies will be destroyed or returned to the originator as soon as possible.
(d) Only members of staff legitimately involved in the work should have access to this information in order to carry out agreed task(s).
(e) Members of staff accessing this information are aware of the conditions under which it is supplied and have an appropriate staff or honorary contract with the organisation they are working for.
(f) The information will only be used for the purpose for which it is supplied.
(g) Information supplied will not be disclosed to any other organisation or individual unless there is an overriding and legally justifiable (statutory) requirement to release the information.

This agreement must be signed by a member of the organisation with sufficient seniority to ensure that these terms are met.