BRIEFING NOTE

Item no. 8

TO: **SOCIAL CARE & INCLUSION SCRUTINY PANEL**
DATE: **14 July 2011**

RE: HEALTHWATCH

Purpose

Healthwatch is being brought to Scrutiny at the request of the Chair to provide the Scrutiny Panel with information to keep them aware of developments with Healthwatch and to provide an opportunity for them to change how these developments are implemented.

Context

The health sector is currently undergoing unprecedented change. This will affect the whole structure and operation of NHS services. As part of this, public engagement and patient involvement in services is changing and the government wants genuinely to give communities a bigger say and more power and influence over services. Specifically, a new Healthwatch organisation will be established, thereby affecting how all health and social care public engagement will operate. Detailed guidance on Healthwatch is still not complete and information is being received from the Department of Health on an ongoing basis. Nevertheless, Walsall is making preparations for bringing current engagement mechanisms together. Specifically, these are:

1. Walsall Local Involvement Network (LINk)
2. MyNHS Walsall
3. Other engagement mechanisms operating through Walsall Manor Hospital

The way in which we hope to bring these organisations together has been set out in a proposal to the Department of Health for Walsall to become a pathfinder for Healthwatch. A copy of this proposal is attached. It requires some intensive development between now and March 2012.

Recommendations

The Scrutiny Panel is requested to:

1. Note ongoing developments with Healthwatch
2. Provide feedback where appropriate

Author

Clive Wright
Director, Walsall Partnership
☎ 01922 654707
wrightclive@walsall.gov.uk

Walsall Partnership

BOARD

SHARED INTELLIGENCE

Monday, 21 March 2011

1 Purpose of the Report

1.1 To give the Board sight of the initial 'overview of key results and ways forward' from the shared intelligence project. The content will form the basis of a presentation made at the meeting which may differ slightly from the attached following further consultation to be undertaken between the dispatch of papers and the meeting itself.

2 Recommendations

2.1 The Walsall Partnership Board is requested to:

i) approve the recommendations as presented at the meeting;
ii) delegate authority to Chief Superintendent Bullas and the Partnership Director to develop an action plan to take forward the recommendations; and,
ii) agree, in principle, to officers from within partner organisations being tasked with implementing the action plan.

3 Background

3.1 At its meeting on 4 November 2010 the Board agreed to support a project to improve the sharing of intelligence between partners. The aims of the project were to reduce duplication and to gain the best understanding possible of demand placed on services provided by partners.

3.2 At the outset it was intended to undertake the project solely using resources from within the Partnership. However, an opportunity arose during December to redirect grant funding secured from the West Midlands Improvement and Efficiency Partnership to support the project. It was felt that an independent assessment using consultants with greater expertise in this area was likely to provide a better outcome.

3.3 Consequently, following a competitive selection process, Professor Paul Foley was appointed to undertake the work. Professor Foley has built up a national reputation in assisting public sector organisations with technology adoption, policy development, regeneration and social inclusion. He is author of 'Intelligent Efficiency' which sets out ten top tips for developing new and effective ways of using information and intelligence to enable councils and their partners to be able to work more efficiently, make better use of resources and save money.

3.4 Over the last two months Professor Foley has made an assessment of the analytical resources employed across the Partnership and whether the intelligence outputs are fit for purpose. He has engaged managers and analysts in this assessment and has provided his initial findings ahead of time for dispatch with papers for the Board meeting on 21 March. Before the meeting views will be sought from:

- Kevin Bullas, the Board Champion for the Shared Intelligence project;
- Lead Officers for the four main Strategic Needs Analyses – Children and Young People, Crime and Disorder, the Local Economic Assessment and the Joint Strategic Needs Assessment (JSNA); and,
- Other Managers and Analysts that will be affected.

3.5 As a result it is possible that the presentation made at the meeting may differ slightly from the attached paper (appendix 1).

Contact Officer:

Tim Ferguson
Head of Partnership and Performance
☎ (01922) 652481
✉ fergusont@walsall.gov.uk

Intelligent Efficiency: Walsall Partnership

Introduction

This paper provides an overview of analytical and intelligence resources and activities for Walsall Partnership[1]. Recommendations are provided about how these can be used more effectively for strategy development and to support Working Smarter. Importantly, the recommendations ensure that the utilisation of analysts and intelligence sharing has a purpose.

The need for local authorities and partnerships to work smarter and more efficiently has probably never been greater. Leaders need information and intelligence to understand what is happening, to develop strategies and to monitor priorities. Partnerships work best when there is a clear vision or agreement on goals to be achieved; this requires shared access to information in order to develop a single understanding of problems, possibilities, solutions and to monitor progress and take corrective action. Intelligence should lead decision making. Many interviewees suggested Walsall was "data rich; but intelligence poor".

The project is not scheduled for completion until 31st March. This paper is therefore an initial viewpoint only.

By developing new and more effective ways of using information and intelligence Walsall Council and their partners will be able to work more efficiently, make better use of resources and save money.

Analytical resources and activities

Walsall Council departments and partners were circulated with a tool to collect details of their analytical resources and the activities of analysts. Ten replies were received.

Replies suggested that Walsall Council has 14 analytical staff. This figure is lower than might have been expected for a Council serving 250,000 residents. A figure of between 22 and 26 analysts was predicted from previous and on-going studies utilising the same methodology. Children's and Adults departments suggested far lower numbers of analysts than might have been have been expected from previous studies. The 14 analytical staff (reported) represent a resource cost of £535,500 (including 'on costs'). In addition those respondents reporting expenditure spent £255,500 on external research. Thus in total the Council analytical budget is £791,000 (if there were 24 analysts this budget would be approximately £1.173million).

Partners (Housing Group, NHS, Fire and Police) reported 16 analysts. This resource is slightly higher than observed in previous studies, but respondents stressed that some of

[1] The project was supported by West Midlands RIEP and involved interviews with fifteen senior council and partnership staff. Additional meetings were held with senior staff and ten analysts.

their analytical resources were also used to undertake activities outside Walsall Borough Council due to non-contiguous boundaries.

In total it is estimated that the partnership has access to between 30 and 40 analysts to support more efficient working.

Council respondents reported producing 44 reports on a monthly, quarterly and annual basis. The inclusion of more fulsome replies from some respondents would probably increase the number of reports to nearer the 70 figure observed in other local authorities of a similar size.

68 per cent of these reports are for Walsall Council internal use, 17 per cent are shared with partners, eight per cent are for national and regional organisations and seven per cent are for citizens or the voluntary sector. The level of internal reporting is relatively high in comparison with previous studies. However, this may reflect the decrease in reporting to higher tiers of government that was advocated after the General Election. Whatever the reason it is evident that the Council and Partnership have the scope to reconsider the production, format and content of 85 per cent of reports produced by the council. This is relevant because many analysts reported that they were preparing unnecessarily detailed reports for many meetings. Interviewees also identified that some reports were too long and sometimes lacked focus and distillation of key points.

It is important to ensure analysts support Working Smarter and do not feed traditional administrative reporting and performance management processes. In Wolverhampton re-examination of just one committee meeting schedule that received one regular report led to analytical savings of 25 person days. This level of saving across nine reports and associated committee meetings would represent a resource saving of one FTE or the release of one person to spend additional time on more productive analytical matters.

Reports processes and duplication

The 44 reports produced by the Council and similar reports produced by partners represent a large input of time and a considerable information resource for all partners. However, it is also evident that these reports (and the big four assessments Local Economic Assessment, Joint Strategic Needs Assessment, Crime Assessment Plan and the Children and Young Peoples Plan) contain large amounts of duplication. Information exchange appears to be infrequent and many analysts appear to spend time re-processing data that has been analysed in previous reports or looking for data and information that other Walsall analysts have already reviewed. Signposting to these reports is poor and it is difficult to find the contents of documents. Better recording of these reports and studies would be advantageous and would prevent a great deal of duplication.

It would also be appropriate to develop a simple modular system of report production for key topics frequently contained in Council and partner reports.

For example the production of a simple but comprehensive catchall report on population (covering trends, forecasts, geographical distribution, variance by age groups, including an

explanation of key issues and why some issues are important) would probably contribute to a large number of reports. The 80:20 rule would probably be relevant. The 'population module' would not meet everyone's needs, but it would prevent many people undertaking the same analysis and reduce the additional analytical work that they might require (the 20 in the 80:20) to a minimum.

It was suggested by one interviewee that approximately 20 modules, updated annually, might be sufficient to create an extensive common understanding of all the key issues concerning the problems and opportunities for Walsall.

An approach that better signposted reports and built up a comprehensive and robust repository of information or reports about key issues would also support issues related to people and expertise development in the next section

Respondents reported that Walsall Council spent £255,500 on external research. Several interviewees identified that some of these studies had survey or citizen consultation elements that could have been jointly commissioned thus sharing costs. IEWM estimates potential savings of more than 30 per cent in collaborative (and / or sub-regional) purchasing agreements.

It was also suggested that some external research was commissioned because policymakers sometimes take more notice of reports if they are generated externally. This is a very expensive way to obtain credibility. External scrutiny of internally produced reports might be a more cost-effective route to add credibility in the future.

Intelligent efficiency will be based on three assets - people, information and systems. There is room for improvement in all three areas in Walsall.

1. People assets

Most interviewees knew an analyst and had access to their usually well established network of contacts and other analysts. But the network is poorly mapped. If someone is away, ill, on holiday (or worse) access to the network (and their knowledge) can be lost. Equally, if someone joins the Council or a partner organisation they are not linked into this network.

Identifying who the analytical 'experts' are and how they can be contacted within the Walsall partnership will help smarter working and help in overcoming the duplication of analytical activities.

If a small number of 'experts' (perhaps 10 to 20) were given a clear designated responsibility to develop the modular report noted in the previous section and they were given support to develop their area of expertise the knowledge base of the Walsall partnership would be extended and become more robust. In addition, by committing some of their expertise to 'paper' in a modular report, fewer problems might arise when experts were not available or left partner organisations.

Some experts will obviously be held in higher repute than others, this was evident in interviews with analysts. But a more transparent form of knowledge sharing through modular reports (with feedback from readers) and greater support to develop expertise should help to address deficiencies.

Better signposting and development of expertise will address the desire amongst some interviewees for better access to intelligence that is "out there, somewhere".

Several analysts noted that they had poorly structured training and career development opportunities. Higher analysts at West Midlands Police have been responsible for overseeing a two-year training and development programming for analysts. This has helped to develop the skills and efficiency of analysts. It has also assisted with the retention of analysts. The average local authority or police analyst has a salary of £25 to £35,000; the private sector offers salaries of £40,000 or more. When an analyst leaves a great deal of corporate information and knowledge can be lost.

There were mixed views about the Walsall Analysts Group (WAG). It was regarded as a good networking model, but many felt it was poor at delivering outputs, despite a desire amongst many members to do something. Analyst networking models that work effectively are usually led by an enthusiastic and committed person who leads the development of a group of people who are at a similar level within an organisation. It is suggested that the group is led by a senior analyst. As well as skills and knowledge development the group could be more productive if it was given the remit (and time) to undertake cross-cutting studies or tasks of relevance to policy makers. The group should also be invited to be more proactive in suggesting on a regular basis areas where research is required to enhance Council activities. This would help to develop the level of dialogue between analysts and policymakers.

2. Information assets

Several interviewees suggested that data has frequently been collected out of habit in Walsall – "we need to release ourselves from the burden of collecting unnecessary information".

There is a trade-off between collecting everything at low quality and what is really useful and maintaining quality. Many analysts surveyed have reported spending between 20 and 30 per cent of their time 'cleaning' data.

Poor data is common in many authorities. It is important to have designated information asset owners. They should be responsible for the upkeep and accuracy of data, and this must be part of their performance review. This will usually be a task for the person overseeing collection or input of the data or their line manager.

Unlike many nearby authorities Walsall does not possess a Local Information System. Walsall Partnership Observatory[2] is useful, but does not possess the full functionality of a system. Systems can be purchased off-the-shelf for as little as £10,000 to £15,000. Thousands of national data sets can be purchased and updated for approximately £5,000 per annum. Local data can also be integrated into systems. A single source of data for members, partners and citizens can offer considerable time savings by reducing time wasted finding (or trying to find) data. It is recommended that Walsall establishes a Local Information System.

However, a Local Information System is not a holy grail. Most members and partnership employees want intelligence not data. The mathematical and analytical skills of many possible users have been questioned during interviews. Simply putting data online does not provide the intelligence that many people want. The goal should be to provide (within limited resources) a local information ***service***, where analysts support those using the online system.

A central resource could be provided to support the development of a local information system, to promote use and to respond to queries from users. Research undertaken for CLG suggests that a system in Walsall (purchased for £25,000) with annual running costs of £40,000 (one analyst [including 'on-costs'] plus £5,000 per annum for data) would 'break even' (in terms of time savings for users) with only 200 users, the system could also achieve pay-back (on the initial investment) within one year[3]. Most systems achieve a user base of 400 to 600 within the first year.

3. System assets

Walsall Council like many other local authorities and partnerships have a highly complex IT landscape with several complete but separate business support systems, which are distributed across a number of departments or authorities. Each system has its own set of products, functionality, and processes and each department frequently has its own support or analytical group.

The complex IT landscape frequently leads to spending more money than required on IT and operations. The structure also negatively affects the ability to identify needs across different departments or authorities and to provide services efficiently. There was a desire amongst analyst interviewees to self-serve from good quality centrally accessible data repositories.

Migration to a single system, with an architecture and processes that fit the business strategy, has enabled private sector businesses such as TalkTalk to reduce IT costs by 50 per cent. New architecture can unify data repositories and automate data distribution, reducing manual steps and running fewer tests.

---

[2] www.walsall.gov.uk/wpo-maps/wpo_interactive_maps.htm

[3] www.esd.org.uk/LIS-value-assessment/Assessment.aspx

Making the transformation work will require the agreement of key stakeholders on the overall vision, as well as their determination to make the changes succeed. This will require input from the IT professionals, but also the commitment and support of the Chief Executive(s) or a champion who should set out the vision for a unified IT landscape. Having management share the vision is critical to success.

Strategy and operations

A number of interviewees suggested that a focus on Working Smarter and lean service provision, stimulated by current economic circumstances, was leading to a focus on operational activities at the expense of strategic direction. Some interviewees suggested that the council and partnership lacked a clear strategic direction or they lacked a clear vision to address Walsall's most pressing problems. They suggested that a focus on delivery obscured wider consideration of whether services (provided or commissioned) were appropriate to meet local needs within resources available. One person commented that "we might be doing things right, but are we doing the right things?"

One manifestation of this is the lack of joint working to address many cross-cutting problems, such as adult care, child poverty and unemployment. For example some were critical that Walsall Partnership had not established a joint commissioning group bound by section 75 of the Health Act 2006. At present, the partners commission mental health and learning disability services separately, rather than together, and in many cases from the same providers.

A study recently found that in Croydon the 200 families making the greatest use of public services were costing the exchequer £300,000 per annum. Where are these families in Walsall? What are their needs? How can the £60m of services they consume be reduced and, if required, provided more efficiently? Is inter-departmental working or service provision across the partnership well enough developed to recognise the problem, to utilize the intelligence required to identify the appropriate families and collectively address their needs? It is this type of more strategic approach that can be lost if there is too much of a departmental or service delivery focus.

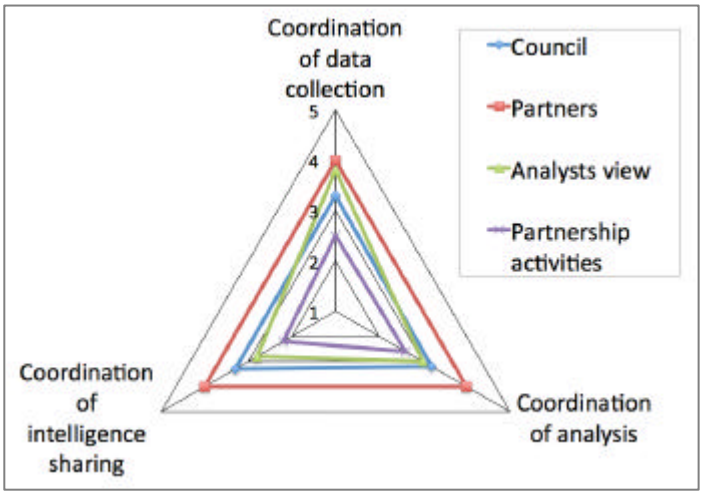
Strategic or cross-cutting approaches ideally require the amalgamation of people with a variety of areas of expertise. For example addressing child poverty has implications for health, education, employment and housing services. It is possible to address these issues by bringing together analysts on a 'task and finish' basis to address specific issues. All interviewees suggested they were happy with this approach.

A more effective longer-term approach is to draw analysts together and create a knowledge hub to inform and provide an evidence base for strategic and cross-cutting operational activities. Private sector organisations create knowledge hubs consisting of analysts at the centre to generate and apply knowledge and to transmit knowledge and organisational goals throughout the organisation. This is the solution favoured by most interviewees in Walsall. However, it must be acknowledge that some were opposed to this approach since it might mean a loss of some analysts from individual departments or organisations in any

realignment. One must acknowledge that analysts working in specific departments generate first hand knowledge of local conditions and specific local circumstances. However, this local knowledge will not be lost if a hub is created, since some analysts will still remain in individual departments or organizations. Indeed, it is even possible that the small number of analysts drawn together to create a knowledge hub might still provide some input to individual departments or organizations.

Some have suggested that a virtual or online hub might be created to enable analysts to collaborate. In the first instance it is suggested that a knowledge hub in Walsall should involve the co-location of analysts at single point at the centre of the partnership or council to support senior executives across the council or partnership to make better informed strategic and operational decisions.

The creation of a knowledge hub will assist with addressing the perceptions held by interviewees about the level of very poor coordination for data collection, analysis and intelligence sharing across the partnership. Partners generally felt their organisations' had "coordinated" analytical activities. Council interviewees felt activities were generally "fragmented". All interviewees agreed that partnership activities were generally "very fragmented".



The knowledge hub should have the task of overseeing and developing corporate knowledge. It should also oversee the streamlining of information and intelligence collection and dissemination to ensure that the right information in the correct format at the right time is provided to all employees. In addition the hub should provide a flexible 'task and finish' resource that can be used to intelligently attack problems and identify and seize opportunities for the partnership or individual departments or partners who have specific requirements for short-term analytical support. These might be cross-cutting problems across a number of departments or areas where local analytical expertise is lacking or in short-supply.

The success of the hub should be measured by ensuring that executives and managers throughout the council or partner organisations find the intelligence inputs provided are relevant to their strategy and policy development activities. At the heart of this goal is the need to enhance communication between executives, managers and analysts.

Several interviewees and analysts noted that some executives and managers do not know what guidance they require or the specific questions they should pose to analysts. It was suggested some did not understand the role and contribution of intelligence in strategy development. This led to no communication, a bland requirement to "tell me everything you know about X", or a request to find evidence to support a particular decision.

Equally it was suggested by a few interviewees that some analysts reports were not challenging enough. Analysts need to see strategic issues as integral to their job and to challenge managers' long-held perspectives, viewpoints and assumptions and demonstrate what 'best practice' solutions are available.

13th March 2011

Recommendations

To achieve many of the efficiency improvements and savings suggested above it is necessary for Walsall partnership and/or the council to develop an Intelligence Strategy. The central goal of the strategy must be to ***get the right information, in the right format, to the right person at the right time***. Many of the constituent elements of an intelligence strategy have been highlighted in this short paper.

Core components will include:-

Reports and reporting methods

- Reconsider the production, format and content of the 85 per cent of reports produced by the council that are only required by the council or partnership.
- Better recording and signposting of current reports and future report production is required.
- Better signposting of future external consultancy commissioning is required to see if costs might be shared with partners or neighbouring authorities.
- Develop a simple modular system of annual report production for key topics frequently contained in Council and partner reports.
- Ensure that all committee and other analytical reports are accompanied by a feedback form that is completed by readers and returned to report authors.

People

- Identifying and then signpost who the analysts are in Walsall Council and partner organisations, identify their areas of expertise are and how they can be contacted.
- Designate a small number of 'experts' (perhaps 10 to 20) and support them to develop their area of expertise and ensure they contribute to the production of annual modular reports.

Information assets

- Appoint designated information asset owners. They should be responsible for the upkeep and accuracy of data, and this must be part of their performance review.

- A Local Information System should be established. The system should play a central role (within limited resources) of providing a local information service. Analysts should provide the human-face to support the online system

System assets

- Analysts should be able to 'self-serve' from good quality centrally accessible data repositories.

Knowledge hub

- A small number of analysts should be drawn together and create a knowledge hub to inform and provide an evidence base for strategic and cross-cutting operational activities.
- In the first instance it is suggested the a knowledge hub should involve the co-location of analysts at single point at the centre of the partnership or council
- The success of the hub will be enhanced by promoting communication between policymakers and analysts to ensure that executives and managers throughout the council or partner organisations find the intelligence inputs are relevant to strategy and policy development activities.

13th March 2011

Walsall Partnership
Overarching Information Sharing Protocol

Version 1.4
May 2011

Document Version Details

Date	Version	Author	Comments
Aug 2010	1.0	LW\NU	
Aug 2010	1.1	NU	Reviewed / added Data Quality section and relevant appendices
Sept 2010	1.2	LW	Added acknowledgment information and included template PSISA to appendices
Sept 2010	1.3	NU	Minor amendments for clarity - WMP
May 2011	1.4	AS	Removal of reference to Local Area Agreement

CONTENTS

1 Executive summary

1.1 This document is an Overarching Information Sharing Protocol ("this Protocol") covering all organisations within the Walsall Partnership. It also represents the organisational approach being adopted by Walsall Metropolitan Borough Council ("the Council"). The list of current organisations covered by this Protocol can be found in section 11. It does not impose any new obligations, but reflects current regulations and legislation.

1.2 This Protocol sets out the agreed standards that staff in within the Council and public, voluntary and independent partner organisations must adhere to. It is intended to complement any existing professional Codes of Practice that apply to any relevant professionals working within these partner organisations.

Acknowledgements

WMBC would like to acknowledge Lambeth Council in the development of this document.

2 Introduction

2.1 It is recognised that effective information sharing is required in order to enable organisations to improve client services, protect the public and respond to statutory requirements. Organisations also recognise the importance of having clear guidelines to follow and ensuring that this information is shared in a secure and confidential manner and in accordance with the law, including the common law of confidentiality, the Data Protection Act 1998, the Human Rights Act 1998 and other related legislation and guidance.

2.2 In this Protocol, all references to personal information / personal data / data / sensitive information / sensitive personal data relate to one or both of the following definitions provided in the Data Protection Act 1998.

Personal data means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

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.

Sensitive personal data means personal data consisting of information as to

(a) racial or ethnic origin of the data subject,

(b) political opinions,

(c) religious beliefs or other beliefs of a similar nature,

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) physical or mental health or condition,

(f) sexual life,

(g) the commission or alleged commission of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

2.3 This Protocol (and appendices) comprises a set of rules that the organisations identified in section 11 agree to comply with when sharing any personal information with another partner organisation. It sets out the standards that staff must follow when sharing personal data to ensure that legislation is not breached and that confidentiality is maintained.

2.4 The sharing of anonymised or purely statistical information is outside of the remit of this Protocol, as the majority of legislation and rules concern only the sharing of personal information. However, the Purpose Specific Information Sharing Agreement template created under this Protocol can be used to form a basis for the sharing of anonymised or statistical information.

2.5 Signatories to this Protocol must be the highest level official within the partner organisation (e.g. Walsall Council's Chief Executive). This high-level commitment is recognition that information sharing is a key strategic objective of the partnership within Walsall.

3 Organisations covered by this protocol

3.1 Section 11 contains a list of the organisations who have signed up to this Protocol.

4 Purpose of the Protocol

4.1 Overarching objectives

4.1.1 To provide a robust framework for the legal, secure and confidential sharing of personal or sensitive information between partner organisation to enable them to meet both their statutory obligations and the needs and expectations of the people who they serve.

4.1.2 The strategic purposes of this Protocol for the sharing of personal or sensitive information are:

a) the delivery of integrated public sector services in line with government initiatives and public expectations,
b) to facilitate the management and planning of cost effective and efficient services; and,
c) to enable parties to this Protocol to review, account for, and learn how to improve what they do.

4.1.3 This Protocol also:

a) Clarifies the legal background on information sharing
b) Outlines the principles that are needed to underpin the process
c) Provides practical guidance on how to share information in a series of supporting procedures
d) Provides a framework within which organisations can develop Purpose Specific Information Sharing Agreements (PSISA) for specific areas of service
e) Includes arrangements for reviewing the use of this Protocol and for responding to breaches of this protocol or any of the PSISAs.

5 Governance and review

5.1 Status of this protocol

5.1.1 This Protocol **(Tier 1)** is the highest level in the protocol structure and applies to all sharing of personal or sensitive information. It contains the general principles of information sharing and the legislative standards that all types of personal information sharing must comply with.

5.2 Walsall Partnership

5.2.1 This Protocol is owned by the Walsall Partnership. Walsall Partnership brings together different parts of the local community - public services, local businesses, community groups, voluntary sector organisations and local people to work together in a co-ordinated way to plan local services, tackle the issues that matter to local people and improve quality of life in Walsall. This protocol sits above the current Safer Walsall Borough Partnership protocol which specifically covers tackling crime and disorder within the borough.

5.3 Safer Walsall Partnership

5.3.1 This Protocol will be used as a key tool to support partner agencies of the Safer Walsall Partnership Board and in this context, for information sharing between the council, the Primary Care Trust, the Police, Probation Service, Fire Service and others.

5.4 Formal approval, adoption and review

5.4.1 This Protocol will be formally signed off by the Chief Executive (or equivalent) for each of the partner agencies.

5.4.2 Formal adoption will follow as soon as 2 or more partner organisations have signed this document. This document then forms the basis for information exchanges between those organisations who have signed up. All partner organisations wanting to share personal data under this Protocol must sign this agreement.

5.4.3 Following implementation this protocol will be reviewed after 6 months. Thereafter it will be reviewed every year or sooner as legislation and guidance dictates. The reviews will be undertaken by the Walsall Partnership in consultation with the Caldicott Guardians and Data Protection Officers of the Partner agencies.

5.4.4 Breaches of this Protocol and subsequent PSISAs will be managed according to the Procedures set out in appendix D - Handling Breaches.

6 Protocols at two levels

6.1 The structure

6.1.1 This Protocol **(Tier 1)** is the highest level in the protocol structure and applies to all sharing of personal or sensitive information. It contains the general principles of information sharing and the legislative standards that all types of personal information sharing must comply with.

6.1.2 The Purpose Specific Information Sharing Agreements (PSISA) represent **Tier 2** of the structure. The PSISAs will specify precisely what information is to be shared, how it will be shared and to whom that information will be given for a particular area of activity. Responsibility for the production of PSISAs rests with the Head of Service (or equivalent) for the relevant service area.

6.1.3 The PSISA must be signed by the relevant Head of Service (or equivalent) for that particular area of work and the Organisation Contact for Information Sharing under that PSISA. The PSISA must comply with the principles set down in this Overarching Protocol. A framework PSISA is contained within appendix E.

7 Legal basis for sharing information

7.1 Understanding the legal framework for information sharing

7.1.1 The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.

7.1.2 It is essential that practitioners sharing information are clearly aware of the legal framework within which they are operating.

7.1.3 The purpose therefore of detailing the law within this Protocol, is to highlight the legal framework that affects all types of personal information sharing, rather than to serve as a definitive legal reference point.

7.2 How to approach questions around information sharing

7.2.1 In order to approach questions around information sharing this Protocol contains useful checklists (see appendices).

7.2.2 Appendix A - Checklist of legal consideration raises some of the questions in a more user-friendly way.

7.2.3 In summary this comes down to:

a) Establishing whether there is power to carry out the function to which the information sharing relates

b) Checking whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of statutory, common law or other provisions

c) Deciding whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim

d) Decide whether the sharing of the data would breach any obligations of confidence

e) Decide whether the data sharing could take place in accordance with the Data Protection Act 1998, with particular reference to the 8 Data Protection Principles.

7.3 Freedom of Information Act (FOIA) 2000 requests

7.3.1 A number of the partner organisations are “public authorities” for the purposes of the Freedom of Information Act 2000 (FOI). This means that they could receive requests for information relating to the information sharing activities under this Protocol or resultant PSISA (e.g. statistics on the amount of data sharing being undertaken or the general nature of the data sharing). The public authority that receives the FOI request must make the other public authority aware of the nature of the request and their intended response.

8 General undertakings by each agency

8.1 A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing information appropriately.

8.2 The sharing of information by organisations under this Protocol (and subsequent PSISAs) will be based on the following principles:

8.3 Commitment to sharing information

8.3.1 Partner organisations recognise that multi-agency working sometimes requires a commitment to sharing personal or sensitive information about service users in compliance with guidance and legislation.

8.4 Statutory duties

8.4.1 Partner organisations are fully committed to ensuring that they share information in accordance with their statutory duties including the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

8.4.2 Partner organisations recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and will adhere to the requirements of Schedule 3 of the Data Protection Act 1998 in respect of such information.

8.5 Caldicott requirements

8.5.1 All organisations recognise the requirements that Caldicott imposes on NHS organisations and Social Services Departments. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements.

8.6 Governance & Duty of confidentiality

8.6.1 Partner organisations recognise the importance of the legal duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are lawful grounds and an overriding justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

8.6.2 Organisations who are party to this Protocol will exercise caution when contemplating the disclosure of personal information relating to a deceased person. Although the Data Protection Act only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.

8.6.3 Organisations who are party to this Protocol will have in place appropriate measures to ensure that the sharing of personal information is conducted within an environment that supports the protection of vulnerable, adults, children and young people, including the use of the relevant vetting and

checking processes for specified staff.

8.6.4 All organisations who are party to this Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

8.6.5 In the event of personal information that has been shared under this Protocol (and subsequent agreements) having or may have been compromised, whether accidental or intentional, the organisation making the discovery will without delay:

i) inform the information provider of the details

ii) take steps to investigate the cause

iii) if appropriate, take disciplinary action against the person(s) responsible.

iv) take appropriate steps to avoid a repetition

v) take appropriate steps where possible to mitigate any impact

8.6.6 On being notified that an individual's personal information has / have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary take action to:

i) notify the individual concerned

ii) advise the individual of their rights

iii) provide the individual with appropriate support.

8.6.7 See appendix D - Handling Breaches for more information.

8.7 Consent

8.7.1 All organisations who are party to this Protocol will consider the option of seeking consent from the individual concerned to share their personal information in accordance with an agreed PSISA. Where this is not obtained or cannot be obtained, it will be necessary to consider which other conditions can be met and /or the application of one of the legal exemptions.

8.7.2 Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential to avoid the need to repeatedly seek consent over minor issues.

8.7.3 In seeking consent to disclose personal information, the individual concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to withhold or withdraw consent.

8.7.4 For further guidance on consent, see appendix C Consent: Guidance notes.

8.8 Sharing without consent

8.8.1 Organisations will put procedures in place to ensure that decisions to share

personal information without consent have been fully considered and comply with the requirements of the relevant law. Such decisions will be appropriately recorded for audit purposes. All relevant staff will be provided with training in these procedures.

8.8.2 For further guidance see appendix C Consent Guidance notes.

8.9 "Need to know"

8.9.1 Where it is necessary and permissible for information to be shared, this will be done on a "need-to-know" basis only. i.e. the minimum information, consistent with the purpose for sharing, will be given.

8.10 Information kept confidential from the service user

8.10.1 Where professionals request that information supplied by them be kept confidential from the service user, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on lawful grounds.

8.11 Specific purpose

8.11.1 Partner organisations will not misuse information that is disclosed to them under the specific purpose(s) set out in the relevant PSISA. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for their general use.

8.11.2 Organisations wishing to use information for any purpose other than that for which it was originally provided, or who wish to disclose that information to any person other than those authorised to receive that information, must attempt to:

i) inform the organisation that provided the information of their intention to use that information for a different purpose, and

ii) Obtain explicit consent from the individual(s) concerned before processing such information (unless this is not practical – e.g. crime prevention purposes).

8.11.3 Organisations who wish to use information that has been provided to them under a PSISA for research or statistical purposes must ensure that policies and procedures are in place to guarantee that such personal information is anonymised and in line with ethical standards.

8.12 Fact / opinion

8.12.1 Agencies who are party to this Protocol will ensure that their staff, who are authorised to make disclosure of personal information, will clearly state whether the information that is being supplied is fact, opinion, or a combination of the two.

8.13 Use of anonymised information where possible

8.13.1 Personal information will only be disclosed where the purpose for which it has

been agreed to share clearly requires that this is essential and appropriate. For all other purposes, information about individual cases that is to be shared will be anonymised.

8.14 Access to information

8.14.1 Individuals will be fully informed about the information that is recorded about them, who may see their information, for what purposes and their right to object to the relevant person within that organisation (see section 15). Under the Data Protection Act they will normally be able to gain access to information held about them and to correct any factual errors that may have been made.

8.14.2 If an organisation has statutory grounds for restricting a person's access to information about themselves, they will normally be told that such information is held and the grounds on which it is has not been provided (unless this would prejudice an investigation or place an individual at risk).

8.14.3 Information that has been provided by another agency under an agreed PSISA may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent must be obtained prior to disclosure:

i) The provider has specifically stated that the information supplied must be kept confidential from the service user

ii) The information contains medical details

iii) The information is legally privileged

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

8.14.5 Where an opinion about an individual is recorded and the individual feels the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and record their disagreement with the recorded opinion.

8.15 Complaints procedures

8.15.1 Partner Organisations shall put in place procedures to address complaints relating to the disclosure of information. Partners must also ensure that service users are provided with information about these Complaint procedures.

8.15.2 In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied / obtained under an agreed PSISA, all agencies who are party to the PSISA will provide co-operation and assistance in order to resolve the complaint.

8.16 To ensure minimum standards for all PSISAs

8.16.1 In order to maintain a consistent approach, all agencies who are party to this Protocol will ensure that any PSISA will follow the framework set out in appendix E.

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

8.17 Disciplinary action

8.17.1 Partner organisations will ensure that contracts of employment and/or relevant policies and procedures include reference to the issue of disciplinary action should staff disclose personal information on a basis which cannot be justified as reasonable in the particular circumstances (taking into account the purpose of the disclosure and any relevant statutes).

8.18 To record information disclosed under these protocols in the following way

8.18.1 Organisations who are party to this Protocol will:

(a) ensure that all personal information that has been disclosed to them under an agreed PSISA will be recorded accurately on that individual's manual or electronic record in accordance with their policies and procedures.

(b) put in place procedures to record not only the details of the information, but who gave and who received that information.

8.19 Storage, transfer and destruction of personal information

8.19.1 Organisations who are party to this Protocol will put in place policies and procedures governing:

(a) the secure storage of all personal information retained within their manual and/or electronic systems

(b) the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

i) Internal and external postal arrangements

ii) Verbally, face-to-face and telephone

iii) Facsimiles (safe haven)

iv) Electronic mail (secure network or encryption)

v) Electronic network transfer

(c) the access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.

(d) the retention and destruction of records containing personal information retained within their manual and/or electronic systems.

8.20 To ensure that staff under this protocol comply with their obligations

8.20.1 Organisations who are party to this Protocol will ensure:

i) that all staff are aware of, and comply with, their responsibilities and obligations with regard to the confidentiality of personal information about people who are in contact with their organisation/agency.

ii) that all staff are aware of, and comply with, the commitment of the organisations/agency to only share information legally and within the terms of an agreed Purpose Specific Information Sharing Agreement.

iii) that all staff are aware of, and comply with the commitment that information will be shared on a need-to-know basis only.

iv) that staff will be made aware that disclosure of personal information which cannot be justified, whether recklessly or intentionally will be subject to disciplinary action.

8.21 To ensure that members of staff are trained to enable them to share information legally

8.21.1 All parties to this Protocol will ensure that employees who need to share personal information under a PSISA are given appropriate training to enable them to share information legally, comply with any professional codes of practice and comply with any local policies and procedures.

8.21.2 Staff who are not directly involved with sharing personal or sensitive information should not be excluded from such training as it is possible that they may come across such information during the course of their duties. It may therefore be appropriate that such employees receive awareness training.

8.22 Data quality and metadata standards

8.22.1 The key to better information to support decision making and accountability lies with the actions that partners take to foster a culture that values the quality of the data that underpins this information. Such a culture must be adopted at the very top of, and pervade, the whole organisation. Suitable assurances of data quality are essential if all parties are to have confidence in the resulting information that is being shared.

8.22.2 In signing up to this Protocol, all parties are confirming that they have arrangements in place to ensure appropriate standards of data quality that support the information they provide. Partners should therefore be able to demonstrate that they have:

i) defined their priorities for data quality;

ii) assessed their arrangements for securing good quality data; and

iii) developed working practices which deliver these objectives.

8.22.3 The standards outlined below in section 8.21.4, (and in further detailed in Appendix E) are as defined by the Audit Commission and are intended to provide a consistent framework and common standards for different

partner organisations to adopt.

8.22.4 To ensure a high and consistent standard of quality, all data supplied should be:

i) Accurate: providing a true account of what they are intended to represent (balanced with a need to provide timely data);

ii) Valid: complying with agreed requirements and definitions;

iii) Reliable: having stable and consistent collection processes over time/place;

iv) Timely: being available promptly and frequently enough to support needs;

v) Relevant: considering the intended purposes and audience;

vi) Complete: presenting a comprehensive picture of the current situation.

These dimensions of data quality are explained in further detail in Appendix E

8.22.5 These standards are based on accepted good practice and should therefore be fully compatible with existing definitions and standards required by individual agencies. As such, they are intended to consolidate, rather than replace, any agreements and standards that partners already have in place. They can also be used as a framework for organisations that may not have any other formal guidance.

8.22.6 Where parties already have their own internal data quality agreements, guidelines or audit arrangements, these should be made available to Walsall Partnership. This will reassure agencies of the quality of one another's information as well as enable good practice to be disseminated.

8.22.7 Alongside the information being provided, parties should supply appropriate metadata (i.e. 'data about the data'). Metadata describes the attributes of the data and information and should help the user to gain a full understanding of how the data was collected, what exactly is being described describe and to assess whether it is fit for the intended purpose. Metadata should therefore help users to understand any limitations in the usefulness of the data and resulting information.

8.22.8 Metadata becomes even more essential where data is being shared outside the organisation. Each PSISA should set out its own specific metadata requirements to be supplied alongside the information being shared. Appendix F provides a core set of standards to build on.

9 Purposes for which information will be shared

9.1 Overview

9.1.1 Information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. However, each agency must have regard to its legal power in

deciding whether they can share information for that particular purpose. The following range of purposes are agreed as justifiable for the transfer of personal or sensitive information between the Partner Organisations as defined within the remit of this Protocol. This list is not exhaustive:

a) Provision of appropriate care services

b) Assuring and improving the quality of care and treatment

c) Improving the health of people in the local community

d) Monitoring, reporting and protecting public health

e) Protecting children, young people and adults

f) Prevention of crime or disorder and the promotion of community safety

g) Supporting communities (geographical or otherwise)

h) Supporting people in need

i) Investigating complaints or potential legal claims

j) Compliance with court orders

k) Managing and planning services

l) Commissioning and contracting services

m) Developing inter-agency strategies

n) Performance management and audit

o) Research

p) Other statutory requirements

9.2 Relevant information

9.2.1 Consideration must be given to the extent of any personal information that is proposed to be disclosed, taking into account the circumstances of the proposed disclosure. It may not be necessary to disclose all information held regarding a service user and only such information as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

10 Agreement

10.1 Indemnity

10.1.1 Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

10.1.2 Parties to this Protocol shall ensure that both the request and the disclosure are compliant with the requirements of the Data Protection Act 1998.

10.1.3 If subsequently it is found that either the request for, or the disclosure of,

information is in contravention of the requirements of the Data Protection Act 1998, the organisation who originally breached the requirements of the Data Protection Act 1998, either in requesting or disclosing information, shall indemnify the other organisation against any liability, cost or expense thereby reasonably incurred. However, this indemnity shall not apply:

a) Where the organisation originally found to be in breach of the Data Protection Act 1998 did not know and, acting reasonably had no reason to know, that it had acted in breach of the Data Protection Act 1998 either in requesting or disclosing information

b) Unless either organisation notifies the other organisation as soon as reasonably practical of any action, claim or demand against itself to which it considers this indemnity may apply, permits the other organisation to deal with the action, claim or demand by settlement or otherwise, and renders all reasonable assistance in doing so.

10.2 The undersigned parties agree to:

10.2.1 Promote good practice in the sharing of personal information by ensuring compliance with the principles, purposes and processes of this Protocol.

10.2.2 Take necessary action to identify and mitigate any breaches of the Protocol and to have established policies and practices for dealing with complaints about the sharing of information.

10.2.3 Ensure that no restrictions are placed on sharing personal information other than those that are specified in this Protocol.

10.2.4 Ensure that Data Subjects are informed of their rights in respect of personal information, including right of access and the complaints procedure.

10.2.5 Develop systems of implementation, dissemination, guidance, training and monitoring to ensure that the Protocol is known, understood and followed by all professionals who need to share personal information.

10.2.6 Establish processes to review the use of this Protocol, in order to ensure that practice is in accordance with the requirements of this Protocol, and to take corrective action as needed.

10.2.7 Develop information processing systems that ensure collected data is complete, accurate, kept up-to-date and relevant.

10.2.8 Ensure that collected data is stored and transmitted securely.

11 Signatories

11.1.1 This protocol will be signed by chief officers of the respective agency organisations on behalf of their organisations:

11.1.2 Signed copies of this document shall be retained by the Council's Data Protection Advisor.

11.1.3 Any Organisation who is not party to this Protocol, but who would want to share information under a Purpose Specific Information Sharing Agreement may do so providing that they agree to comply with the terms of this Protocol, insofar as it is relevant to the information sharing to which that Purpose Specific Agreement relates.

ORGANISATION	NAME	DESIGNATION	DATE SIGNED

12 APPENDIX A - Checklist of legal considerations

Below is a non-exhaustive list that is of relevance to information sharing

12.1 Purpose

12.1.1 This is meant as a guide to assist in determining how to establish the legal basis for data sharing:

12.2 Vires issues

12.2.1 Is the existing information that is to be shared subject to any statutory prohibitions whether express or implied?

12.2.2 Even if there are no relevant statutory restrictions, do the bodies sharing the data have the vires to do so? This will involve careful consideration of the extent of express statutory, implied statutory and common law powers (see appendix B for further detail on statutory powers).

12.2.3 If there is no existing legal power for the proposed data collection and sharing, then, can the individual's consent to the disclosure be obtained?

12.3 Human Rights Act issues

12.3.1 Is Article 8 of the European Convention on Human Rights (ECHR) engaged i.e. will the proposed data collection and sharing interfere with the right to respect for private and family life, home and correspondence? If the data collection and sharing is to take place with the consent of the data subjects involved, Article 8 will not be engaged.

12.3.2 If Article 8 of the ECHR is engaged, is the interference

a) in accordance with the law;

b) in pursuit of a legitimate aim;

c) a proportionate response to the problem;

d) necessary in a democratic society?

12.4 Common-law duty of confidence issues

12.4.1 Is the information confidential i.e. does it:

a) have the necessary quality of confidence

b) was the information in question communicated in circumstances giving rise to an obligation of confidence?

c) has there been an unauthorised use of that material?

12.4.2 Consider also whether the information has been obtained subject to statutory obligations of confidence. If the data collection and sharing is to take place with the consent of the data subjects involved, the information will not be confidential.

12.4.3 If the information is confidential is there an overriding public interest that justifies its disclosure? The law on this aspect overlaps with that relating to Article 8 of the ECHR.

12.5 Data Protection Act issues

12.5.1 Does the DPA apply i.e. is the information personal data held on computer or as part of a “relevant filing system” or an “accessible record”?

12.5.2 If the DPA applies, can the requirement of fairness in the First Data Protection Principle be satisfied?

12.5.3 Can one of the conditions in DPA Schedule 2 be satisfied? Of particular relevance to public sector data sharing are the requirements in paragraph 5 that relate to public functions; and the requirement in paragraph 6, that involves a balance between the interests of the data subject and the interests of the body that shares and/or that receives the data.

12.5.4 If the data are sensitive personal data can one of the conditions in Schedule 3 also be satisfied? Paragraph, 7 which is in similar terms to paragraph 5 of Schedule 2, may be applicable.

12.5.5 Can the requirement of compatibility that is in the Second Data Protection Principle be complied with?

12.5.6 Do any of the exemptions that are set out in the Data Protection Act apply?

12.5.7 Seek advice from your organisation’s Data Protection Officer/Legal Advisor if unsure.

13 APPENDIX B - Relevant legislation

13.1 List of legislation and other guidance potentially relevant to data sharing activities

Below is a non-exhaustive list that is of relevance to information sharing:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- The Mental Health Act 1983
- The Children Act 1989 (sections 17, 27, 47 and Schedule 2)
- The Children Act 2004 (sections 10, 11 and 12)
- The NHS & Community Care Act 1990
- The Access to Health Records Act 1990
- The Carers (Recognition & Service) Act 1995
- The Crime & Disorder Act 1998
- The Health Act 1999 (section 31)
- The Health and Social Care Act 2001 (Section 60)
- The Local Government Act 2000 (section 2)
- The Local Government Act 1972 (section 111)
  The Education Act 1996 (sections 10 and 13), The Education Act 2002 (section 175)
- The Learning and Skills Act 2000 (sections 114 and 115)
- The Crime and Disorder Act 1998 (section 115)
- The NHS confidentiality code of practice
- The Civil Contingencies Act (2004) Part 1 and supporting regulations.
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005

13.1.1 Some of the legislation is defined in greater detail below. For further advice on this legislation and other relevant professional guidance contact your organisations designated officer.

13.2 Introduction

13.2.1 Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the organisation to enable it to carry out a particular function.

13.2.2 In many instances legislation tends to use broad or vague statements when it comes to the matter of sharing personal information, for example: the organisation is required 'to communicate, or will co-operate with' without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998.

13.2.3 The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable

information (Personal Data). In general, recorded information held by public authorities about identifiable living individuals will be covered by the Data Protection Act 1998. It is important to take account of whether the information is held in paper records or in automated form (such as on computer or on a CCTV system): some of the provisions of the Data Protection Act 1998 do not apply to certain paper records held by public authorities. Broadly speaking, the eight data protection principles set out in Schedule 1 to the Data Protection Act 1998, and discussed further below, will apply to paper records held in a "relevant filing system" or an "accessible record", but not to other paper records.

13.2.4 The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, providing that the necessary conditions of the Act can be met, sharing is perfectly legal.

13.3 Administrative Law

13.3.1 The principles of administrative law regulate the activities of public bodies; these principles are mainly enforced by way of claims for judicial review in the courts. The courts do not generally review the merits of public law decisions but consider the legality, rationality or procedural propriety of decisions made by public bodies. The rules relating to illegality are most relevant to data sharing: a public body may not act in excess of its powers. If it does act in excess of its powers, then the act is said to be 'ultra vires'. Acts within a public body's powers are said to be 'intra vires'. Under the Human Rights Act 1998, an act of a public authority may be unlawful on the basis that it is contrary to the European Convention on Human Rights (ECHR). Where questions involving the Convention are involved, the Court will need to consider the merits of the decision more closely than would be the case where the traditional administrative law principles are involved.

13.3.2 Local authorities derive their powers entirely from statute and cannot act outside those limited statutory powers. Most of these statutory powers relate to specific local authority functions. In addition to these specific powers, section 111 of the Local Government Act 1972 provides that local authorities are empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions. Section 2 of the Local Government Act 2000 confers a wide (but not unlimited) power on local authorities to promote the well-being of their area.

13.3.3 There is no general statutory power to disclose data, and there is no general power to obtain, hold or process data. As a result, it is necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied. Express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked. Alternatively it may be possible to rely on section 111 of the 1972 Act or section 2 of the 2000 Act as a basis for data sharing.

13.3.4 The starting point in relation to implied powers or in relation to section 111 of the 1972 Act must be the power to carry out the fundamental activity to which data sharing is ancillary. If there is no power to carry out that fundamental activity then there can be no basis for implying a power to share data or for relying on section 111 of the 1972 Act.

13.3.5 A statutory power must be exercised for the purpose for which it is created. If it is not, the exercise of the power will be ultra vires.

13.4 Administrative powers

13.4.1 Express statutory powers: Express statutory powers can be permissive or mandatory. Express permissive statutory powers (or gateways) to share data include section 115 of the Crime and Disorder Act 1998 (which allows persons to share information with relevant authorities where disclosure is necessary or expedient for the purposes of the Act) and regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (which, among other things, permits the Secretary of State to make particulars in the vehicle registration register available for use by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention). Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995, which makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 6 of the Audit Commission Act 1998, which imposes a legal obligation on the Council to provide relevant information to the Audit Commission.

13.4.2 Local authorities are only able to do what is expressly or by implication authorised by statute. The following statutory powers are relevant, in addition to the specific powers mentioned above:

a) Section 111 of the Local Government Act 1972, which provides that a local authority has power to do anything, which is calculated to facilitate, or is conducive or incidental to, the discharge of any statutory functions.

b) Section 2 of the Local Government Act 2000, which provides that a local authority has power to do anything likely to achieve the promotion or improvement of the economic, social or environmental well-being of the area.

13.5 Data Protection Act 1998

13.5.1 The key principles of the Data Protection Act are:

i) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions in schedule 3 of the Act.

ii) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).

iii) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).

iv) Personal Data shall be accurate and kept up to date.

v) Personal Data shall not be held for longer than is necessary.

vi) Processing of Personal Data must be in accordance with the rights of the individual.

vii) Appropriate technical and organisational measures should protect Personal

Data.

viii) Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient.

13.5.2 With few exceptions, the Data protection Act 1998 requires anyone processing personal information to notify (register) with the Information Commissioner.

13.5.3 The registration details include the type of information held, the purpose of use and who the information may be disclosed to. It is therefore essential that anyone considering sharing personal information establishes that their registration covers who they may disclose information to, or what information they may collect (when receiving shared information). If their registration does not cover these matters adequately, amendments must be registered with the Information Commissioner.

13.5.4 The first and second principles of the Data Protection Act are crucial when considering information sharing. In essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should only be used for a purpose(s) compatible with the original purpose.

13.5.5 Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully – For personal information to be processed lawfully, one of the conditions in Schedule 2 must be met. For sensitive personal information, one of the conditions in Schedule 3 must also be met.

13.5.6 Sensitive information, as defined by the Act, includes information concerning a person's physical or mental health; sexual life; ethnicity or racial origin; political opinion; trade union membership; criminal record or details of alleged offences etc.

13.5.7 In order for there to be no misunderstanding, on anyone's part, it is always advisable for the 'collector' of the information to ensure that the person is made fully aware of why the information is needed, what will be done with it, who will have access to it, their rights and if appropriate seek to inform consent of the individual concerned before sharing that information.

13.5.8 There are circumstances where information can be shared even if informed consent has not been given. These include the following:

i) Section 29 of the Act permits disclosure for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure.

ii) Disclosure is also permitted where information has to be made public, or where disclosure is required by law.

13.5.9 For the purposes of the common law duty of confidentiality, if there is no informed consent, this is the point where the need for confidentiality would have to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests. See the more detailed discussion of confidentiality, below.

13.5.10 For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered. See the more detailed discussion of Article 8, below.

13.5.11 The Data Protection Act gives individuals various rights in respect of their own personal data held by others, namely the right to:

i) access their own information (subject access request).
ii) take action to rectify, block, erase or destroy inaccurate data.
iii) prevent processing likely to cause unwarranted substantial damage or distress.
iv) prevent processing for the purposes of direct marketing.
v) to be informed about automated decision taking processes.
vi) take action for compensation if the individual suffers damage.
vii) apply to the Information Commissioner or the court to have their rights under the Act enforced.

13.5.12 Section 7 of the Act, gives an individual the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic).

13.5.13 Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions (e.g. section 7(4) and the exemption provided by section 30 of the DPA).

13.5.14 The Act provides the holder of the information a limited number of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the Act.

13.5.15 The Data Protection Act 1998 does not apply to personal information relating to the deceased person.

13.5.16 The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from section 3.1.(f) which continues to provide a right of access to the health records of deceased person made by their personal representatives and others having a claim on the deceased's estate.

13.5.17 In all other circumstances, disclosure of records relating to the deceased person should satisfy common law duty of confidence.

13.5.18 Schedule 2 of the Data Protection Act 1998 specifies conditions relevant for the processing of any personal data, namely:

i) The data subject has given his/her consent to the processing, or
ii) The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract, or
iii) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, or
iv) The processing is necessary to protect the vital interests of the data subject.
v) The processing is necessary for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions

of a public nature exercised in the public interest by any person, or

vi) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

13.5.19 Schedule 3 of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data, namely:

i) The data subject has given his/her explicit consent, or the processing of sensitive personal data is necessary:

ii) By right or obligation under law, or

iii) To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual or,

iv) In the course of legitimate activities of specified non-profit organisations, with extra safeguards, or

v) Information already publicly released by the individual.

vi) For Legal, judicial, government or crown reasons, or

vii) Medical purposes, or

viii) To monitor equality of opportunity, or

ix) By order of the Secretary of State.

13.5.20 Statutory Instrument 2000/417, provides additional circumstances where sensitive personal data may be processed.

13.6 Human Rights Act 1998 and European Convention on Human Rights

13.6.1 The Human Rights Act 1998 (the HRA) gives effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). In general, it is unlawful under the HRA for a public authority to act inconsistently with any of the Convention rights.

13.6.2 Article 8.1. of the European Convention on Human Rights (given effect via the Human Rights Act 1998), provides that *"everyone has the right to respect for his private and family life, his home and his correspondence."*

13.6.3 This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.

13.6.4 Article 8.2 of the European Convention on Human Rights provides *"there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

13.6.5 In the event of a claim arising from the Act that an organisation has acted in a way

which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s) to have taken a particular course of action:

i) that it has taken these rights into account;
ii) that it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
iii) if there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
iv) (if qualified rights) whether the organisation has proceeded in the way mentioned below. *"Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act".*

13.7 Crime and Disorder Act 1998

13.7.1 The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

13.7.2 Section 115 of the Act provides a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the Crime and Disorder Act. This power does not over ride other legal obligations such as compliance with the Data Protection Act (1998), the Human Rights Act (1998) or the common law duty of confidentiality.

13.7.3 Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service, fire brigades or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.

13.7.4 Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the organisation that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

13.7.5 All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

13.7.6 A duty of confidence arises when one person (the "confidant") is provided with information by another (the "confider") in the expectation that the information will only be used or disclosed in accordance with the wishes of the confider. If there is a breach of confidence, the confider or any other party affected (for instance a person whose details were included in the information provided) may have the right to take action through the courts.

13.7.7 Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

13.8 Exemptions to the duty of confidentiality

13.8.1 The duty of confidence is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed. These are as follows:

- Disclosures with consent. If the person to whom the obligation of confidentiality is owed (whether an individual or an organisation) consents to the disclosure this will not lead to an actionable breach of confidence.

- Disclosures which are required or allowed by law. "Law" in this context includes statute, rules of law, court orders etc.

- Disclosures where there is an overriding public interest (e.g. to protect others from harm).

13.8.2 The courts have generally taken the view that the grounds for breaching confidentiality must be strong ones.

13.8.3 The duty of confidence only applies to information from which an individual can be identified, 'person identifiable information', and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

13.8.4 Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

13.9 Caldicott Principles

13.9.1 Although not a statutory requirement, NHS and Social Care organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:

i) Justify the purpose(s) for using personal information.

ii) Only use personal information when absolutely necessary.

iii) Use the minimum amount of personal information that is required.

iv) Access to personal information should be on a strict need to know basis.

v) Everyone with access to personal information must be aware of his/her responsibilities.

vi) Everyone with access to personal information must understand and comply with legislation that governs personal information.

13.10 Access to Health Records Act 1990

13.10.1 Within the governance structures and processes of healthcare organisations, Practitioners have been given professional accountability to protect specific 1st and 3rd party statements. This may include clinical assessments, diagnostics and results as well as sections of sensitive care plans and progress notes.

13.11 The Children Act 2004

13.11.1 The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children. The key event, which led to these proposals for fundamental change, was the death of Victoria Climbie. This demonstrated that there were major flaws within the systems and structures for safeguarding and ensuring the welfare of children and young people.

13.11.2 Main provisions of the Act:

a) A duty on agencies to co-operate to improve the well being of children and young people
b) A duty to safeguard and promote the welfare of children
c) A power to set up a new database with information about children

13.12 Summary of the Children Act 2004

13.12.1 The following is a brief account of the key parts of the Act that specifically relate to the Change for Children programme in England.

13.13 Children's Services in England – Part 2

13.13.1 Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.

13.13.2 Section 11 creates a duty for the key agencies who work with children to put in place arrangements to make sure that they take account of the need to safeguard and promote the welfare of children when doing their jobs.

13.13.3 Section 12 allows further secondary legislation and statutory guidance to be made with respect to setting up indexes that contain basic information about children and young people to help professionals in working together to provide early support to children, young people and their families. Case details are specifically ruled out of inclusion in the indexes.

13.14 Civil Contingency Act 2004 – Part 1

13.14.1 This deals with information sharing between responder bodies, as identified in the Act, as a distinct duty under the Act and as a means of achieving other duties under the Act, and is summarised below:

- Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation.

- There are various types of information. Information may be suitable for some audiences, but not for others. Also, the circulation of information can be limited to certain classes of organisation or individual.

- In most instances, information will pass freely between responders, as part of a more general process of dialogue and co-operation.

- Information may also be accessible from open sources, and responders should endeavour to use this route as well.

- However, a formal system exists to request information in circumstances where that is necessary.

- Not all information can be shared. Responders may claim exceptions in certain circumstances (and, as a result, not supply information as requested).

- Exceptions relate to sensitive information only. Where the exceptions apply, a responder must not disclose the information.

- Readers of this document are advised to read Chapter 3 the Guidance Notes to the Civil Contingency Act 2004.

14 APPENDIX C - Consent: Guidance notes

14.1 Consent

14.1.1 In the past consent has all too often either been assumed or implied. Unfortunately, when something goes wrong it has been very difficult to prove if consent was actually given. It is therefore recommended that the consent sought should be explicit and appropriately recorded.

14.1.2 In order to facilitate the sharing of personal information (without specific statutory grounds) careful consideration should be given to obtaining explicit consent whenever possible, regardless of the person's age.

14.1.3 For consent to be valid it must be:

Fully informed – the individual is aware of what information will be shared, with whom and for what purpose.

Specific – a general consent to share information with "partner organisations" would not be valid. Specific means that individuals are aware of what particular information we will share, who with and for what purpose.

A positive indication by the data subject – the provision of opt outs on forms would therefore not obtain the consent of an individual.

Freely given – the individual is not acting under duress from any party.

14.1.4 The person giving the consent must also have the capacity to understand what they are consenting to.

14.1.5 Consent may be given non-verbally, orally or in writing. In order to avoid any confusion or misunderstanding at later date, non-verbal or oral consent should be witnessed and the details of the witness recorded.

14.1.6 To give valid informed consent, the person needs to understand why their information needs to be shared, what type of information may be involved and who that information may be shared with.

14.1.7 The person should also be advised of their rights with regard to their information, namely:

i) The right to withhold their consent.

ii) The right to place restrictions on the use of their information.

iii) The right to withdraw their consent at any time.

iv) The right to have access to their records.

14.1.8 As well as discussing consent with the person, it is seen as good practice that the person should also be given such information in another required format e.g. different language, Braille.

14.1.9 In general once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent.

14.1.10 If a person makes a voluntary and informed decision to refuse consent for their

personal information to be shared, this decision must be respected unless there are sound legal grounds for disclosing without consent (see 14.8 below).

14.1.11 A person, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusal, their wishes must be respected unless there are sound legal grounds for not doing so.

14.1.12 If a person refuses or withdraws consent, the consequences should be explained to them, but care must be exercised not to place the person under any undue pressure.

14.1.13 In the PSISAs detail must be provided (in response to Question 10) on when and how often individuals are reminded of the fair processing notice (and in effect given the chance to withdraw the consent that they have previously provided).

14.1.14 New consent will be required where there are to be significant changes to:

a) the personal data that will be shared,

b) the purposes for which it will be shared, or

c) the partners involved in the sharing (I.e. the proposed data sharing is not covered by the original fair processing notice – see 14.1.6 and 14.1.7 above).

14.2 Capacity to consent

14.2.1 For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process.

14.3 Young Persons

14.3.1 Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.

14.3.2 The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent.

14.3.3 It should be seen as good practice to involve the parent(s) of the young person in the consent process, unless this is against the wishes of the young person.

14.4 Parental Responsibility

14.4.1 The Children Act 1989 sets out persons who may have parental responsibility, these include:

i) The child's parents if married to each other at the time of conception or birth;

ii) The child's mother, but not the father if they were not so married, unless the father has acquired parental responsibility via a court order or a parental responsibility agreement, or the couple subsequently marry;

iii) The child's legally appointed guardian;

iv) A person in whose favour the court has made a residence order in respect of the child;

v) A local authority designated in a care order in respect of the child:

vi) A local authority or other authorised person who holds an emergency protection order in respect of the child. (Note: Foster parents or guardians do not automatically have parental responsibility)

14.4.2 Whilst, under current law, no-one can provide consent on behalf of an adult in order to satisfy the Common law requirement, it is generally accepted by the courts that decisions about treatment, the provision of care, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

14.5 Obtaining Consent

14.5.1 For consent to be valid a number of criteria must be satisfied (see Consent 14.1.3 above). In order for consent to be obtained lawfully it is essential that all persons who may be expected to obtain consent for the sharing of personal information receive appropriate training and that under normal circumstances only those employees who have received training and been approved by management should seek consent.

14.6 Disclosure of Personal Information

14.6.1 The passing of personal information without either statutory power or the consent of the person concerned, places both the organisation and the individual member of staff at risk of litigation.

14.6.2 It is therefore essential that all agencies who are party to the Overarching Protocol have in place policies and procedures governing who may disclose personal information and that such policies/procedures are communicated to all of their employees.

14.7 Disclosure with consent

14.7.1 Only staff who have been authorised to do so should disclose personal information about an individual service user.

14.7.2 Prior to disclosing personal information about an individual, the authorised member of staff should check the individual's file/record in order to ascertain:

a) that consent to disclose has been given, and

b) the consent is applicable for the current situation, and

c) any restrictions that have been applied.

14.7.3 On the first instance of disclosure with respect to the particular situation, the person making the disclosure should notify the recipient if consent has been given for the disclosure and any specific limitations the individual has placed on their consent.

14.7.4 Disclosure of personal information will be strictly on a need to know basis and in accordance with any Purpose Specific Information Sharing Agreement.

14.7.5 All information disclosed should be accurate and factual. Where opinion is given, this should be made clear to the recipient.

14.7.6 On disclosing personal information to another organisation, a record of that disclosure should be made on the individual's file/record, this should include:

a) When the disclosure was made
b) Who made the disclosure
c) Who the disclosure was made to
d) How the disclosure was made
e) What was disclosed

14.7.7 The recipient of information should record:

a) The details of the information received
b) Who provided it
c) Any restrictions placed on the information that has been given

14.8 Disclosure without consent

14.8.1 Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

14.8.2 There are exceptional circumstances in which a service user's right may be overridden, for example:

a) If an individual is believed to be at serious risk of harm, or

b) If there is evidence of serious public harm or risk of harm to others, or

c) If there is evidence of a serious health risk to an individual, or

d) If the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime.

e) If instructed to do so by a court

14.8.3 All agencies should designate a person who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person should hold sufficient seniority within the organisation with influence on policies and procedures. Within the health and social care agencies it expected that this person will be the Caldicott Guardian.

14.8.4 If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

14.8.5 A record of the disclosure will be made in the service user's case file and the service user must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed. If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection

work) where it may not be appropriate to inform the service user of the disclosure of information. This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the service user of such disclosure. In many such situations it will not be a case of never informing the service user, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the service user's case file, clearly stating the reasons for the decision, and the person making that decision.

14.8.6 In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

14.8.7 All agencies who are party to this Overarching Protocol should set in place policies and procedures that deal specifically with the sharing of information under emergency situations e.g. major disaster.

14.8.8 If disclosure is made without consent, the person making the disclosure must:

a) Advise the recipient accordingly.
b) Record the full details of the disclosure that has been made, including the reason why the decision to disclose was taken (statute or exemption); who made the disclosure and to who it was disclosed to.

14.8.9 The recipient of information that has been disclosed without consent should record:

a) The details of the information received.
b) Who provided it
c) Any restrictions placed on the information that has been given e.g. not to be disclosed to the service user'.
d) That the information was provided without consent and the reason why (if known).

14.9 Recording Consent

14.9.1 All agencies should have in place a means by which an individual or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

14.9.2 The consent form should indicate the following:

a) Details of the organisation and person obtaining consent.
b) Details to identify the person whose personal details may/will be shared.
c) The purpose for the sharing of the personal information.
d) The organisation(s) / agency (ies) with whom the personal information may / will be shared.
e) The type of personal information that will be shared.
f) Details of any sensitive information that will be shared.
g) Any time limit on the use of the consent.
h) Any limits on disclosure of personal information, as specified by the

individual.

i) Details of the supporting information given to the individual.

j) Details of the person (guardian/representative) giving consent if appropriate.

14.9.3 The individual or their guardian/representative, having signed the consent, should be given a copy for their retention.

14.9.4 The consent form should be securely retained on the individual's file/record and that relevant information is recorded on any electronic systems used in order to ensure that other members of staff are made aware of the consent and any limitations.

15 APPENDIX D - Handling Breaches of the Overarching Purpose Specific Information Sharing Agreement

15.1 Reporting Breaches of the Protocol

15.1.1 All breaches are to be logged, investigated, and the outcome noted. The logs will be examined as part of the review process.

15.1.2 The following types of incidents will be logged:

- Refusal to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- Disclosure of information to members of staff who do not have a legitimate reason for access
- Non-delivery of agreed reports
- Inappropriate or inadequate use of procedures e.g. insufficient information provided
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements.

15.2 Breaches noted by members of staff:

15.2.1 A member of staff working on behalf of any organisation party to this protocol who becomes aware that the procedures and agreements set out in the protocol (or subsequent agreements) are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the protocol.

15.2.2 The manager should record the issue and check whether the concern is justified. If the manager concludes that the protocol is being breached, he or she should first try to resolve it informally. If the matter can be resolved in this way, the outcome should be noted and forwarded to the designated person for that PSISA who should file the details in a ‘breaches log’.

15.3 Breaches alleged by a member of the public:

15.3.1 Any complaint received by, or on behalf of, a member of the public concerning allegations of inappropriate disclosure of information will be dealt with in the normal way by the internal complaints procedures of the organisation who received the complaint: Any disciplinary action will be an internal matter for the organisation concerned.

15.3.2 In order to monitor adherence to and use of the protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information is passed by the officer designated to deal with breaches of the PSISA. The designated officer should report any complaints of this nature to the equivalent officer in each organisation.

15.3.3 All alleged breaches of the protocol, whether proven or not, should be analysed as part of the formal review of this protocol

16 APPENDIX E – Dimensions of Data Quality

16.1 The Audit Commission has identified six key characteristics of good quality data, as detailed in its publication *Improving information to support decision making: standards for better quality data* (Audit Commission, 2007).

ACCURACY

Data should be sufficiently accurate for their intended purpose, representing clearly and in enough detail a true account of what is happening: reported information that is based on accurate data provides a fair picture of performance and should enable informed decision making.

Data should be captured once only, although they may have multiple uses. This helps ensure that all information is based on consistent set of data. Accuracy is most likely to be secured if data are captured as close to the point of activity as possible.

The need for accuracy must be balanced with the importance of the uses for the data, and the costs and effort of collection. For example, it may be appropriate to accept some degree of inaccuracy where timeliness is important. Where compromises are made on accuracy, the resulting limitations of the data should be clear to their users. This must be a judgement determined by local circumstances, and is not generally appropriate in the case of the data supporting published performance indicators.

VALIDITY

Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions; performance data must follow the NIS guidance or any locally agreed definitions.

This is necessary to ensure consistency between reporting periods and with similar organisations, measuring what is intended to be measured.

Where proxy data are used to compensate for an absence of actual data, or there is no prescribed definition, bodies must consider how well these data are able to satisfy the intended purpose. In the case of data to be shared between partners, prior agreement should be reached over what data and collection process will be most appropriate in relation to the outcome being measured.

RELIABILITY

Data should reflect stable and consistent data collection, calculation, recording, analysis and reporting processes across collection points and over time –continuing to follow the agreed definitions and guidance each time performance data are produced.

Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or

methods.

TIMELINESS

Data should be captured as quickly as possible after the event or activity and must be available for the intended use with a reasonable time period, i.e. be as close to 'real-time' as is feasible.

Data must be available promptly and frequently enough to support information needs and to influence service delivery and management decisions. Similarly it must be timely enough to allow for corrective action to be implemented where needed.

RELEVANCE

Data captured should be relevant to the purposes for which they are used. By considering the intended uses and audience at the onset, collection processes will be more likely to result in data that is fit for purpose and adds value to the decision making process. This may entail periodic review of requirements to reflect changing needs.

It may be necessary to capture data at the point of activity which is relevant only for other purposes, rather than for the current intervention. Quality assurance and feedback processes are needed to ensure the quality of such data.

COMPLETENESS

Data should be complete and comprehensive to ensure they provide a full picture of the current situation and allow a full assessment to be made (for example of performance against targets). Where datasets are incomplete and/or could be misleading, this should be made clear to enable appropriate judgements to be made about the use of the data. Data requirements should be clearly specified based on the information needs of the body and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recoding of certain data items.

17 APPENDIX F – Data Specification and Metadata Template

THIS MAY NEED REVISION – BASED ON REQUIREMENTS FOR AGGREGATED DATASETS, PERSONAL DATA WILL HAVE ITS OWN SUPPLY/RETENTION REQUIREMENTS

SUPPLY & RETENTION INFORMATION	
DATA	Title of dataset
CONTACT PERSON	A named data analyst/position within the organisation
CONTACT DETAILS	Address, email and telephone number
DATE OF SUPPLY	Estimated dates of supply for 1 year
FORMAT IN WHICH SUPPLIED	As case data or pre-aggregated to local boundaries In Excel /Word/CSV etc
FREQUENCY OF UPDATES	How frequently the data is available
DATA STORAGE SECURITY REQUIREMENTS	Level of security required to safely store this data
PERSONS HAVING ACCESS TO THE DATA	Names of the people allowed to view the raw data
WHEN PUBLISHED, THE MINIMUM NUMBER OF OCCURENCES IN A CATEGORY	To avoid disclosure, data will not be published for an area if there are a small number of occurrences. This threshold will be set by the partner organisation.
RETENTION PERIOD OF SUPPLIED DATA	Length of time which the raw data can be retained for
METADATA	
COVERAGE	
Spatial	The geographical area the data covers (e.g. ward, borough)
Temporal	Dates covered (e.g. 2004 or 1999-2001)
DEFINITION	
Description	Description of the data
Calculation	If data are provided as a rate or percentage, include details of the calculation including the denominator
DATE	
Date produced	Date this set of data was produced
Date modified	Date this set of data was modified if applicable
Reason for modification	Reason for re-releasing the data

18 APPENDIX G – Purpose Specific Information Sharing Agreement Template

PURPOSE SPECIFIC INFORMATION SHARING AGREEMENT

The Agreement

The Sharing of Personal and Sensitive Personal Data between [ ] and [ ] for the purposes of [name of project or work for which this PSISP relates]

Document Version Details

Version	Date	Author	Comments

This document requires the following approvals

Date	Version	Name	Role

Introduction

General

See the "Walsall Partnership Overarching Information Sharing Protocol", Section 6 for an overall description of the Information Sharing two tier approach and the different elements.

In order to share appropriate information between partners there must be a lawful, defined and justifiable purpose(s) which supports the effective delivery of a policy or service that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This in turn must be supported by robust business processes.

Scope of this Purpose Specific Information Sharing Agreement (PSISA)

1.2.1 This PSISA is the second element of the information sharing framework. It is aimed at an organisations 'operational management/practitioner' level and it will define the relevant business processes which support information processing/sharing between two or more organisations for the specific purpose of [name of project or work for which this PSISP relates].

1.2.2 Those Managers/Practitioners/Designated Persons negotiating this PSISA are required to complete Sections 2 to 14 inclusive of this document.

1.2.3 This PSISA is supplementary to the Overarching Protocol (Tier 1), which must be consulted when drawing up this agreement.
See the "Walsall Partnership Overarching Information Sharing Protocol", Section 6 for an overall description of the Information Sharing two tier approach and the different elements.

1.2.4 Partner organisations may belong to a variety of differing PSISA.

1.2.5 Partners may use the information disclosed to them under a PSISA only for the specified purpose(s) set out in that PSISA document. They may not regard shared information as intelligence for the general use of their organisation unless they have defined and agreed this purpose within the PSISA and have informed their respective service users of this use.

1.2.6 Wherever this PSISA impacts, or has a dependency, on another PSISA then details of these must be entered into the Table at Section 2 of this document.

Parties to this PSISA

1.2.4 The parties to the PSISA are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document (See this Document Annex 1). This list, along with the details of each organisation's 'Designated Person(s)' as shown on the 'DAP' and at Annex 2, will be updated and reissued on a regular basis.

1.2.5 Any party to this PSISA who is not already a party to the Overarching Protocol agrees to comply with the terms of the Overarching Protocol insofar as it is relevant to the information sharing under this PSISA.

1.2.6 By signing this document all of the parties agree to accept and implement this PSISA and to adopt the statements and procedures contained within it.

1.2.7 Any purported breaches of, or other complaints about, this agreement will be dealt with in accordance with the processes described at Appendix D of the Overarching Protocol.

2 Links to Other PSISA:

PSISA Title	Effective From	Effective To	Lead organisation	Contact Details

3 Is the information to be shared "personal data" or "sensitive personal data" as defined in the Data Protection Act 1998?

Personal Data – YES or NO

Unless the information to be passed is entirely anonymised or statistical, the answer to this will probably be "yes". However, even if it is anonymised or statistical, you should give careful consideration to the possibility that an individual could nevertheless be identified from it, or other information held by the Data Controller – e.g. if it provides statistics on the ethnicity of crime victims in a limited geographical area it might inadvertently identify someone from an uncommon ethnic group in that locale.

Sensitive Personal Data – YES or NO

Information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

4 Whose information is to be shared (i.e. which service users?)

Data Subjects are: LIST

This agreement covers information relating to any person(s) living with the borough of Walsall whose personal data falls within the parameters detailed at section 6 of this agreement.

5 Why will the information be shared?

Information will be shared under this agreement in order implement the main principles of [name of project or work for which this PSISA relates].

In summary, these principles will help to achieve improvements to the physical and economic environment and improvements to the health and wellbeing of those who live and work within Walsall

The proposed lead objectives and areas of main focus and effort for [name of project or work for which this PSISA relates] are:

List

Explain why information will be shared

6 What information will be shared?

Detail the information that will be shared under this PSISA

The data fields requested have been paid due consideration, and are proportionate to the needs of this programme and are as follows:

- List the data to be shared

7 To whom will the information be disclosed (i.e. which organisations and/or practitioners)?

It is proposed that Data, from the all parties to this agreement will be disclosed to parties involved in [name of project or work for which this PSISA relates]. This will include, [name organisations].

The raw data will be stored securely (see section 12) [specify location of where data will be stored], and access will be limited to [specify who will have access to the data being shared]

8 Legal basis for sharing information

To be able to share data lawfully, the legal basis for doing so needs to be considered. The following pieces of legislation have been identified as possible grounds to facilitate the legal sharing of personal and/or sensitive data.

The following legislation has been considered for the purposes of data sharing within the [name of project or work for which this PSISA relates].

[Delete legislation as appropriate to this PSISA]

Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act 1998 provides a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the Crime and Disorder Act. This information can be both personal data and depersonalised information.

There is soon to be a new duty placed on certain authorities to share depersonalised in line with the Section 17A of the Crime and Disorder Act 1998 (in schedule 9(5) of the Police and Justice Act 2006).In this section it states that 'a relevant authority is under a duty to disclose to all other relevant authorities any information held by the authority which is of a prescribed description, at such intervals and in such form as may be prescribed…."prescribed" means prescribed in regulations made by the Secretary of State...'.

Some of the information that is to be shared under this agreement will fall under this new duty to share information.

Human Rights Act 1998 9 (HRA) & Children Act 1989 (CA)

Where issues are raised in relation to impairment of a child's health or development, or child abuse, the Children Act may provide statutory authority to share information. Article 8 of the HRA authorises interference '.... for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others'.

CA 1989 s.17 obliges local authorities to safeguard and promote the welfare of 'children in need' and so far as is possible to, promote the upbringing of children within their families, through the provision of a range of services.
CA 1989 Schedule. 2 paragraph. 7 requires every local authority to take reasonable steps to reduce the need for care proceedings and to reduce youth offending.

Children Act 2004

Section 10 establishes a duty on local authorities to cooperate and to work with other stakeholders, (including sharing information), to assess local needs to formulate a Children and Young People's Plan (CYPPs) reflecting local and national priorities for improving outcomes. Section.17 provides the statutory basis for CYPPs the requirements for which are found in the CYPP Regulations 2005. These regulations provide statutory power for extensive information sharing.

Interference (including through inter-agency information sharing) can be justified to protect a child's life (in accordance with Article 2. HRA) or to prevent abuse and torture. However interference should be kept to the minimum possible and where consent is not obtained, the parents /child should be informed of what actions will be taken unless it is inappropriate to do so.

Local Government Act 2000

S.2(1) affords every local authority power to do anything they consider likely to achieve certain aims, including promotion or improvement of social well-being in their area subject to the provisions of other statue such as DPA 1998, HRA 1998 and the common law duty of confidentiality.

Data Protection Act 1998

The Data Protection Act 1998 (DPA) regulates the processing (e.g. use, disclosure and storage) of personal data. The Act requires that for this disclosure and further use of personal data to take place, one condition within schedule 2 (of the DPA) must be satisfied and in the case of "sensitive personal data", one condition within schedule 3 (of the DPA) must also be satisfied. The information to be shared relates to services being accessed by residents and / or other identified needs of these residents and as such will include both personal and sensitive data as prescribed under the DPA.

There are a number of conditions contained within schedule 2 of the DPA, one of which is consent. However, the individuals consent is not required to share information under this agreement where one of the other requisite conditions is met. The condition that can be satisfied is that which is contained within paragraph 6 (1). This condition states that:

"The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject."

Alternatively the condition contained within paragraph 5(d) of schedule 2 could also be relied upon for the sharing of personal data under this agreement. This condition applies where

"the processing is necessary for the exercise of any other functions of a public nature exercised in the public interest".

For the processing of sensitive personal data without consent, at least one of the conditions in found in schedule 3 of the DPA or the one of the conditions found in Data Protection (Processing of Sensitive Personal Data) Order 2000 needs to be satisfied.

It is considered that the processing is necessary for administering justice, or for exercising statutory or governmental functions**.**

In addition, the processing is required to discharge functions which protect members of the public from certain conduct which may not constitute an unlawful act, such as incompetence or mismanagement.

Being able to satisfy one of the above conditions for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately, in line with the principles of the Data Protection Act and other relevant law.

9 Consent

The consent of individual data subjects is not mandatory to enable the sharing of personal data under this agreement, in line with the purpose of the agreement and the conditions specified in 8 above.

10 Notification of Service Users and what information they are told about the data sharing exercise.

Detail the "fair processing notice" (See Appendix C – 14.1.6 and 14.1.7of the Overarching Information Sharing Protocol) that individuals are given about data sharing under this agreement. Also outline how and when this notification is provided to individuals. If applicable, outline the circumstances where the Service User will not be told about the information sharing.

If the consent is due to last for a lengthy period of time, detail at what points/how often an individual will be reminded of the fair processing information and given a subsequent chance to "opt out" having previously given consent.

11 How and when may information be shared

Give specific details of the method by which information will be shared.
How will the information be transferred between services?
For regular flows of information give detail on, the process for requesting the information and the roles of the people involved in the information sharing.
Also give specific details on the triggers to information sharing that takes place where the disclosures are on a case by case basis.

12 How will shared information be recorded and held?

What measures will be taken to ensure a record is kept of the information shared? (by the recipient and provider)

How will the information be stored by the receiving partner and what are the physical and technical security arrangements they have in place?

13 Who else can access this information?

Access to any personal information covered by this agreement will be limited strictly to a "need to know" basis. Any party not signatory to this PSISA will not be allowed access to any personal information.

Discuss any possible vetting arrangements e.g. CRB? And controls in place to ensure data is not inappropriately disclosed

14 How long will this information be stored for and how will it be disposed of?

The [name of project or work for which this PSISA relates] is scheduled to run for a period of [ ]
The information shared will be held for the duration of this period or for as long as is necessary to achieve the aims and objectives of the programme. The data will then be securely deleted / destroyed.

15 Validity of this agreement

This agreement is valid for and during the delivery of the [name of project or work for which this PSISA relates] only.

Purpose Specific Information Sharing Agreement
In respect of *(Insert Title)*

DECLARATION OF ACCEPTANCE & PARTICIPATION
Signed by, for and on behalf of:
Page 1 of

Organisation	
Name	
Position	
Contact Details **Phone No** **E-mail**	
Signature	
Date	

Organisation Contact for Information Sharing under this PSISA	
Position	
Contact Details; i.e. **Phone No** **E-mail**	
(DPA98)Registration No & Date of Renewal	

Appendix H

Purpose Specific Information Sharing Agreement
(Insert PSISA Title)
List of Signatory Organisations & their Designated Persons

Page of

PARTNERSHIP MEMBER	DESIGNATED PERSON & POSITION	CONTACT DETAILS Telephone Number & EMail Address

Please insert, complete and print additional sheets where required.

Walsall Council

NHS Walsall

SERVICE SPECIFICATION SCHEDULE 1
Healthwatch Walsall
The Provision of Service to host and support the activities of Walsall Healthwatch
Block Purchase Contract

1.0	Purpose
	The purpose of the service is to support, facilitate and host Walsall Healthwatch. The role of local Healthwatch is determined as part of the legislation passed by the Health and Social Care Bill 2011. The Health and Social Care Bill 2011 passed changes to the Department of Health (DOH) guidance section 221 (2) of the Local Government and Public Involvement in Health Act 2007 and Schedule 1 of the Health and Social Care Act 2008 to establish and form local Healthwatch organisations as proposed in the White Paper *Equity and excellence: Liberating the NHS (July 2010)*. The legislation requires the development of Local Healthwatch to reform and augment the responsibilities of LINks (Local Involvement Networks).
	Local Healthwatch will be the local consumer champion across health and social care and will: • Retain LINks' existing responsibilities to promote patient and public involvement and to seek views on services which can be feed back into local commissioning; • Have continuing rights to enter and view provider services; • Continue to comment on changes to local social care and health services; • Continue to champion the NHS constitution and the patient rights it sets out; • Report concerns about the quality of local health and social care services to Healthwatch England. Local Healthwatch will be able to do this independently of their local authority. Ref: IDEA.gov.uk Improvement and Development Agency – National and Local Healthwatch Local Healthwatch will have representation on the Health and Wellbeing Board. Within Walsall the local Healthwatch will also replace or act as the body which facilitates MyNHS Walsall.

2.0	Objectives
	To empower citizens and promote independence.
	To provide citizens with information for them to make informed decisions
	To promote health well-being.
	To promote social inclusion
	To ensure the needs of citizens are taken into account with regards to service delivery and provision.
	To improve the quality of provision of social care and health services
3..0	**Service Description**

	Governance arrangements and accountability: The service will work to the identified arrangements as approved by Walsall Partnership developed during 2011 to host Walsall Healthwatch. This will include: ** If not already developed in the transition year support Walsall Healthwatch to develop and adopt appropriate Terms of Reference/Constitution which meet all required statutory obligations and cover: • Accountability arrangements • Membership • Rules of representation (representative groups) • Conflicts of interest • Relationship • Methods of engagement • Communication pathways • Dispute/resolution procedures • Decision-making arrangements • Meeting local COMPACT arrangements • Clear aims and objectives to meet the requirements of the local Healthwatch as identified by Healthwatch England and to determine priorities identified by the members of Walsall Healthwatch • Processes in place to consider how to influence and contribute to the priorities identified by Walsall's Joint Strategic Needs Assessment and Walsall Health and Wellbeing Board Supporting the governance of the group and reporting arrangements to Healthwatch, England and Walsall Health and Wellbeing Board ensuring the terms of reference/ constitution fulfil statutory requirements.
	Reporting: The service will support Walsall Healthwatch to produce reports and information as appropriate for Healthwatch England, Walsall Health and Wellbeing Board and its members.

	Work programme: Support Wasall Healthwatch to follow a planned work programme to review quality standards of Health, Public Health and Adults Social Care Services in Walsall. Support Walsall Healthwatch to develop and implement a process to effectively prioritise the work programme which will be based on priorities identified by the members, informed feedback and to comply with requirements identified by Healthwatch England. Develop the work programme to consider also the feedback from Walsall Area Partnerships and the priorities identified by Walsall's Joint Strategic Needs Assessment. Work with Walsall Healthwatch to develop processes to be available to and to act as a link to other representative organisations to enable consultation and involvement within Walsall and to scope the potential for a wider remit.
	Membership: Develop and maintain a system to implement varied levels of membership and involvement with Walsall Healthwatch and produce a menu or pathway of involvement clearly showing the options for involvement from one off individual concern to full engagement as a member of the Walsall Healthwatch Board (group/individual – board member or available for occasional telephone/postal/e-survey). Maintain and update a comprehensive membership listing. Planned approach to promote and gain members and raise awareness of the role of Walsall Healthwatch and how citizens in Walsall can get involved.
	Support to members: Identify competencies required for Walsall Healthwatch members to administer related tasks. Identify local expertise which can be utilised where a representative group has become affiliated with Walsall Healthwatch. Identify training for and provide training to ensure Walsall Healthwatch members have competencies to meet the priorities of Walsall Healthwatch. Keep members informed of Walsall Healthwatch activities through updated web pages, face book and when requested hard copies of information.

	Practical arrangements: Venue provision Premises/office staffed reception, etc. Telephone lines, etc. Opening hours Clear detail of support service and how it supports Healthwatch Facilitation to support engagement Development of Walsall Healthwatch Web page and Facebook, service information – leaflets, newsletters, etc.
	Advocacy, support and advice service: Part of the remit identified for Walsall Healthwatch includes providing advocacy, support and advice to citizens in Walsall about Health and Adult Social Care Services. The service will: Develop a system to be able to provide an advocacy, advice and complaints service with identified processes clearly showing how the service through Walsall Healthwatch will support and assist an individual to make a complaint about services they receive, how advocacy will be provided or sourced to support an individual to make choices about the health and adult social care service they need. This will include option of one to one discussion, web enquiries, face book posts, letter and telephone enquiries to make contact.
	Partnership working arrangements: Listing of all other agencies, etc. and how they will link up.
4.0	**SERVICE ELIGIBILITY CRITERIA**
	The service will support Walsall Healthwatch to ensure all citizens in Walsall can participate and be actively involved in ensuring local priorities about the provision of NHS/Public Health/Adult Social Care Services are recognised.
5.0	**PERFORMANCE/ CONTRACT MONITORING**

	In accordance with the Joint Commissioning Unit Adults and Social Care Contract Management Framework.
6.0	**CONTRACTED STAFF**
	The service will support, and host Walsall Healthwatch through delivery of xxx hours provided by: Staffing levels:
7.0	**STAFF SUPERVISION & APPRAISAL**
	Written records should be kept. Staff appraisals should be conducted on a six-monthly basis.
8.0	**STAFF TRAINING REQUIREMENTS**
	Staff will receive the following training listed below

	Identify any required competencies.

Walsall Partnership

WALSALL HEALTHWATCH PATHFINDER

Proposal

May 2011

1.0 Purpose

1.1 This proposal responds to a joint letter from David Behan (Director General Social Care, Local Government and Care Partnerships) and Joan Saddler (National Director, Public and Patient Affairs) inviting local authorities to submit proposals to become a Healthwatch pathfinder.

1.2 In setting out our proposal we have been cognisant of the Healthwatch Transition Plan, addressing this document whilst also taking advantage of local circumstances and opportunities.

2.0 Theme of this Proposal

2.1 The Healthwatch Transition Plan and the joint letter referred to above requires Healthwatch pathfinders to address the new roles, over and above the roles previously delivered by LINks. This proposal has two inter-linked themes as set out in the table below:

No.	Theme	How Delivered
1	Strengthening Voice	1/ Connecting Walsall LINk with the 14,000 strong MyNHS Walsall membership scheme and its Parliament. A phased approach will focus on connecting LINk, My NHS Walsall, local Patient Participation Groups (PPGs) and the responsibilities of the Hospital Trust, as it moves towards Foundation status, with Area Management and service user groups in the local authority. These key partners are sustainable and funded. Connecting these groups broadens the range of consumer voices heard in Walsall, avoids duplication, provides a greater impact through the consolidation of effort and clarifies how those interested can participate. 2/ Using the highly credible 14,000 strong MyNHS Walsall membership scheme and its parliament, combined with Walsall LINk, to place elected nominees onto the Health and Wellbeing Board. (Note: Walsall is poised to be a Health and Wellbeing pathfinder). 3/ Integrating the Healthwatch pathfinder into Area Partnerships (local structures where communities, rather than the State, lead on local issues), widening the network

		to non-traditional and harder-to-reach groups. 4/ Through Area Partnerships encouraging co-production of solutions and services. (Note: Health work-streams led locally are already established in Area Partnerships).
2	Empowering Healthwatch to be More Accountable	1/ Feeding in data from Healthwatch consultation into the intelligence creation process – a new shared intelligence unit operating across partners (see appendix 1). 2/ Integrating Healthwatch into the Joint Strategic Needs Assessment (JSNA) process. 3/ Providing Healthwatch with data and intelligence so that they are equipped to influence commissioning and decision making within the Health and Wellbeing Board and with commissioners.

3.0 Introduction/Context

3.1 The changes in the health sector generally present Walsall with some very exciting opportunities. NHS Walsall (PCT) have established MyNHS Walsall as a comprehensive health engagement mechanism, with over 14,000 members actively participating and with an elected health parliament which already has direct influence on service providers.

3.2 We have already been working towards Walsall Healthwatch by exploring how we might connect up the MyNHS Walsall membership scheme and parliament with Walsall LINk. This would create Walsall Healthwatch as an integrated and powerful independent champion for the public on health and social care matters, with a significant, diverse and influential membership. As well as these key stakeholder groups and member organisations we have been developing the linkages with other funded and sustained mechanisms – the Patient Participation Groups, the Hospital Trust and Walsall service users' forums – to complement and further strengthen Healthwatch in Walsall. My NHS Walsall is already working with GPs to make sure that each practice has a Patient Participation Group (PPG) to provide patients with a voice in their practice. Work is also underway to strengthen communications links and networking between the PPGs in Walsall and between other local patient involvement forums.

3.3 Further, we have been investing locally in Area Partnerships better to understand our customers and how to meet their needs in localities of Walsall. Area Managers provide the opportunity for Healthwatch to link to local structures and communities, widening the network to non-traditional and harder-to-reach groups providing a more representative consumer voice. One of our six Area Managers is seconded from NHS Walsall and this provides a platform for enabling the Healthwatch network to be extended beyond the usual participants to traditionally excluded communities. We have already established several health-related work-streams where local communities are working to solve local issues, rather than rely wholly on State intervention.

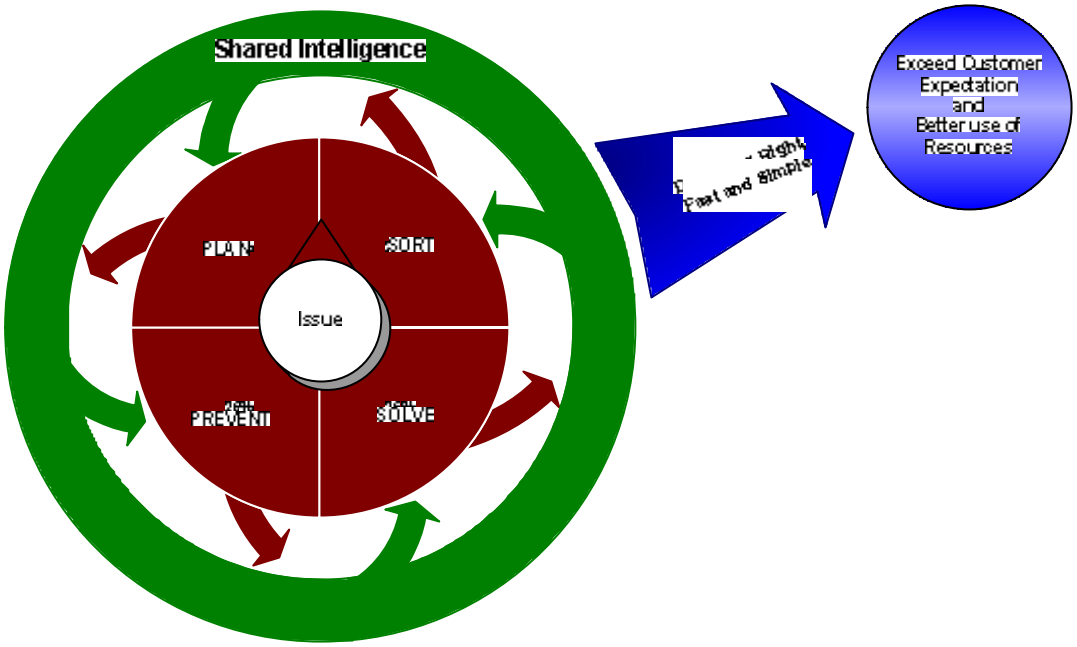
3.4 At the more strategic level we have developed a data-sharing protocol to enable important data held in separate places to be combined to form intelligence (see appendix 2). The customer voice is an important element of this data. Our next step is to bring strategic analytical processes together from separate organisations into one shared intelligence unit, so that safe and appropriate data sharing, and producing intelligence, can occur in real time. The key analytical products of the Joint Strategic Needs Assessment (JSNA), Economic Assessment (Local Economic Plan), Children's Plan and Community Safety Plan will be produced jointly. Integrating Healthwatch into this process will enable them to understand the issues and better represent a wider public.

4.0 Operating System

4.1 *Working Smarter* is Walsall Council's programme and operating system for delivering efficiencies whilst also delivering better services, by understanding customer needs. The principles of our operating system are to be more customer-focused in the design of services and allocation of resources. The consumer voice, provided by Healthwatch is an important element of the strategic intelligence that will be developed and brought to influence commissioners.

4.2 This operating model works at four levels where problems are either solved directly or referred to the next level:

Level 1 SORT	frontline workers are empowered to fix simple problems;
Level 3 SOLVE	more complicated problems are fixed using a team-based approach, potentially involving multiple services and partners
Level 3 PREVENT	processes are redesigned to avoid problems repeating themselves;
Level 4 PLAN	anticipated future demand requires strategic priorities to be set in a way that allows demand to be met.



4.3 This operating model will be applied to all council operations including Healthwatch. This means that Healthwatch has the potential to become a powerful influence across the whole system of council and other partner operations, such as the JSNA, as it drives data and intelligence, scrutinises and effectively channels advice and awareness to have most impact. Utilising the strength of the data and intelligence combined with the wider consumer voice, the front line experience of what local people think, will enable the Healthwatch Board to make robust decisions.

5.0 Walsall Healthwatch Pathfinder Transition Plan

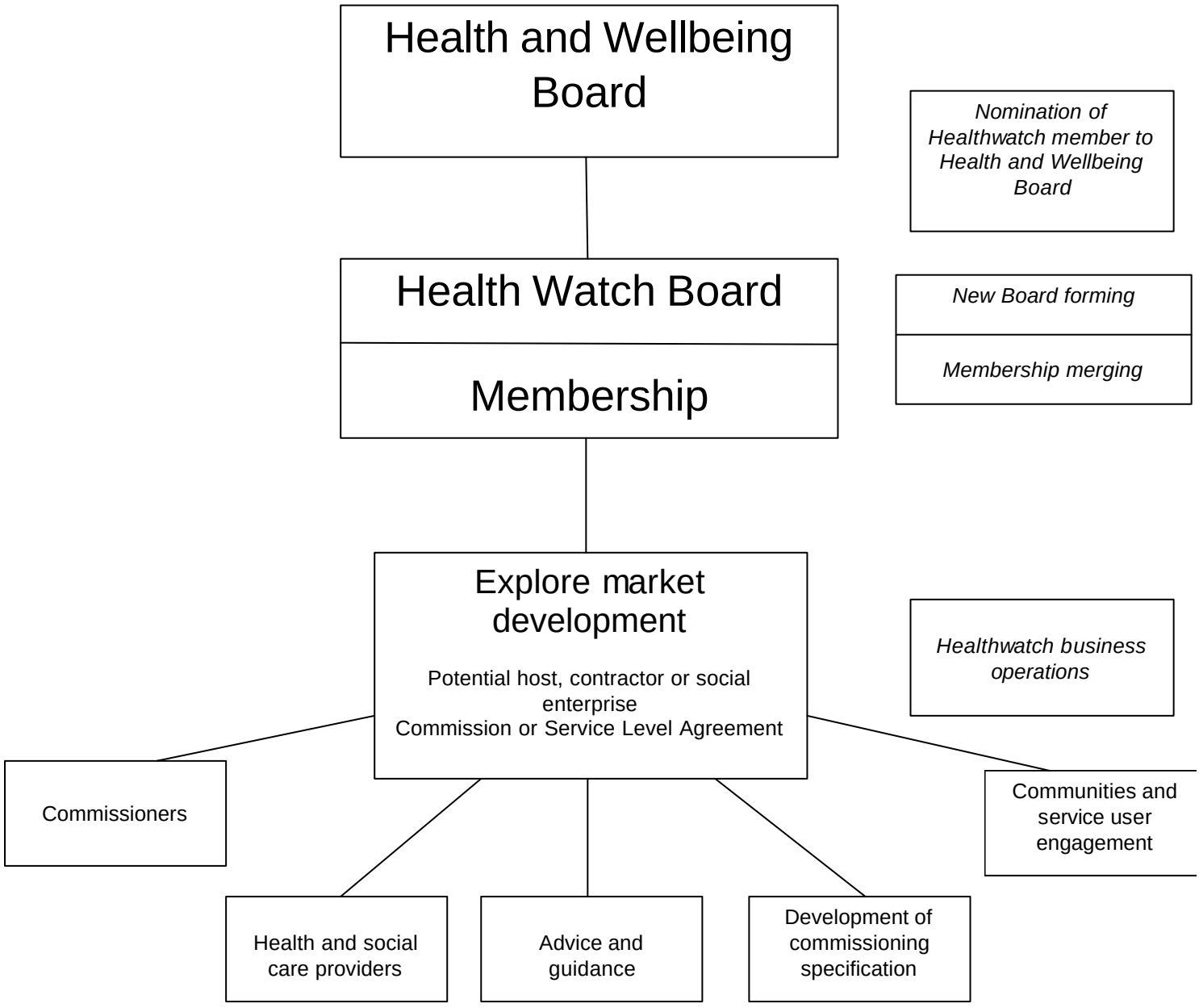
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Assessing Readiness												
Stakeholder meeting every 2 weeks												
Vision for Walsall Healthwatch agreed												
National tools applied												
Pathfinder jointly proposed												
Work plan agreed and implemented												
Strengthening Voice												
Merging LINk and MyNHS Walsall membership												
Broaden awareness and breadth of membership												
Elect Board and Health & Wellbeing Board representative												
Area Partnerships (six areas covering Walsall)												
Explore establishing local Healthwatch in the six areas												
Join local health working groups into Healthwatch												
Plan local advice, guidance and awareness												
Agree strategy to consult and engage harder-to-reach communities and extend Healthwatch voice												
Market Development												
Explore market development												
Commissioning												
Legislation and guidance reviewed												
Outline Healthwatch commissioning specification												
Commissioning specification developed												
Healthwatch Legal Form												
Potential legal forms considered												
Healthwatch constituted as legal entity												
Advice and Advocacy – new duties												
Existing advice and advocacy mapped												
Advice and advocacy planned												
Advice and advocacy implemented												
Monitoring Arrangements												
Outline monitoring arrangements agreed												
Links to CQC developed												

Monitoring arrangements finalised												
Health and Wellbeing Board												
Shadow Board developed												
Expectations of Healthwatch established												
Healthwatch nominee agreed												
Evaluation and Learning												
Resources to capture learning agreed												
Local peer groups established and meeting												
Monthly reports produced												
Participation in DoH action learning sets												
Evaluation planned in detail												
Peer review												
Evaluation report produced												

6.0 Communication Flow

6.1 The Walsall Healthwatch Transition Plan identifies how we see development of Healthwatch during this year of 2011. Critical to this is developing the voice of consumers and so integrating this voice into forums where it needs to be heard is a key task. The joining of the 14,000 members of MyNHS Walsall is a very exciting element of our proposal and is the essential activity taking place between now and July. Walsall's proactive approach to the transition of LINk and Healthwatch and our further exploration, as part of the pathfinder, for the connecting of a wider consumer voice has been welcomed particularly by the transitioning PCT who, as the strategic Black Country cluster, are keen to ensure that statutory duties are acquitted efficiently and effectively.

The following diagram explains how we expect communication to flow.



7.0 Commissioning Specification

7.1 To support our initial model of Walsall Healthwatch structure (see section 6.0) a draft specification has been developed (see appendix 3). This specification would be used to commission the support from a host that Healthwatch will require. This specification will be further developed during the pathfinder process as identified in our commissioning plan.

8.0 Monitoring and Evaluation / Sharing Learning

8.1 If our proposal is successful, we see this as an opportunity to engage with other Healthwatch pathfinders and to share learning.

8.2 As part of this learning we would wish to engage in the Action Learning Sets as described in the Department of Health Transition Plan.

8.3 In addition to the above, we would propose to work closely with other local pathfinders. It would be helpful if peer monitoring, review and evaluation could be established locally to reduce costs and enhance learning and this would be our preferred option. Alternatively, we would engage an independent monitoring, review and evaluation process.

8.4 We are mindful of the critical relationships and change currently taking place within Health, for GP Commissioners, Health and Wellbeing Boards and Foundation Trusts and will ensure relationships continue to be built between these parties in Walsall to support a secure transition from shadow organisations and that there is an alignment of monitoring, evaluation and learning as implementation progresses.

8.5 We would also wish to develop a relationship with the Care Quality Commission to further establish how Healthwatch can be properly empowered to deliver its functions of monitoring and evaluating services.

Contact Officer:

Clive Wright
Director, Walsall Partnership
☎ (01922) 654707
✉ wrightclive@walsall.gov.uk