


Protocol for Sharing Information between Children's Trust agencies working for Children and Young People in Worcestershire

A dark silhouette of a person riding a skateboard, positioned behind the text 'People in Worcestershire'. The background features stylized blue clouds and a rainbow at the bottom.

Amendment history

<i>Version No.</i>	<i>Date</i>	<i>Reason for Amendment</i>
0.1	09/02/09	Initial draft and concepts
0.2	19/02/09	First working draft
0.3	25/03/09	Second draft to incorporate DChS comments
0.4	15/04/09	Third draft to incorporate SDM: Q&P comments
0.5	27/05/09	Final draft to include comments from ChSLT
0.6	15/06/09	Comments incorporated from WCC Legal Services, PAB and WSCB
0.7	05/10/09	Approved version incorporating final comments from JCB
0.8	02/12/09	Final additions/amendments from Partner Agencies
1.0	01/04/10	Published version

Document Control Note:

This document has been subject to Worcestershire County Council's Equality Impact Assessment (EIA) screening process. As a result of the process, it was decided that a full EIA was not necessary.

This Information Sharing Protocol will be monitored by Worcestershire County Council's Information Governance Group.

If you have any queries about the document, the EIA screening process or would like more information about how this will be monitored, please contact Luke Willetts, Operational Manager: Performance Development in Children's Services (lwilletts@worcestershire.gov.uk).



Worcestershire Council for
Voluntary Youth Services



Bromsgrove
District Council
www.bromsgrove.gov.uk



Contents

1. Purpose	5
2. Scope	5
3. Out of Scope	5
4. Statement on safeguarding	6
5. Partner agencies covered by this protocol	6
6. Relationship of this protocol to other protocols	7
7. Legal basis for information sharing	8
8. Reasons for sharing information	9
9. Processes for sharing information	10
9.1 General	
9.2 Informing individuals of the use of their data	
9.3 Confidentiality	
9.4 Consent	
9.5 Quality of information	
10. Security arrangements	12
11. Processes for informing and guiding staff about the arrangements	13
Appendix 1 – Signatories of this information sharing protocol	14
Appendix 2 – Table of Legal Powers under which signatories can share information	15
Appendix 3 – Guidance on issues around the legal framework of information sharing	19
Appendix 4 – Glossary of Terms	24

1. Purpose

Information sharing is key to the Government's goal of delivering better, more efficient public services that are coordinated around the needs of the individual
[DCSF Information Sharing: Pocket Guide \(HM Government, 2008\)](#)

The purpose of this protocol is to provide the framework and to facilitate the sharing of information between agencies, groups and individuals having responsibility for delivering services for children and young people in Worcestershire.

Partner organisations in the Worcestershire Children's Trust demonstrate that by signing this Protocol, they are committed to fair and lawful data sharing in order to safeguard and promote the well-being of children and young people.

Organisations involved in providing services to children and young people have a legal responsibility to ensure that their use of personal information is lawful, and that the individual's rights are respected.

2. Scope

This protocol is intended to formalise:

- the organisational requirements to share data about children and young people by the organisational signatories of this document:
- the sharing of information and data about individual children and young people and their families, between practitioners
- the sharing of bulk information/datasets containing no personal details

Technical detail:

- *individual data subject information (covered by the Data Protection Act 1998).*
- *demographic or generic data (covered by the Data Protection Act 1998). This data should not be used to make decisions regarding individuals.*
- *non-personal aggregate data e.g.*
 - *Data about people that has been aggregated in such a way that makes it impossible to identify individual details*
 - *Data that does not refer to people, but instead to organisations, projects etc.*

3. Out of Scope

This protocol does not cover information sharing that relates to more specific functions/services. These types of information sharing agreements will sit at a 'Tier3' level; please refer to page 7 of this protocol for more details about the framework and Tier system of the Worcestershire Standard for Sharing Personal Data.

This protocol is not intended to cover information sharing between an agency/organisation and a third party (e.g. member of the public/journalist).

Therefore this protocol does not cover the specific responsibilities regarding Freedom of Information, Subject Access Request and Complaints legislation. All organisations should have additional arrangements/processes in place to ensure they are compliant with the legislation within these areas.

4. Statement on safeguarding

[Worcestershire Safeguarding Children's Board](#) are dedicated to making a difference by improving the wellbeing of children and young people and ensuring that they are adequately safeguarded and protected from harm.

This is established in the [Children and Young People's Plan](#): one of the ten priorities is to: 'Ensure that all children and young people are safe, and protected and support those who are at risk of harm and neglect'.

Information sharing is a key component of ensuring that our children and young people are safe from harm. The law allows the sharing of personal information related to individuals when it has not been possible to obtain consent where there is sufficient 'public interest'.

Public interest:

You may lawfully share confidential information if this can be justified in the public interest, even if you do not have consent to share it. Seeking consent should be the first option. However, where consent cannot be obtained or is refused, or where seeking it is inappropriate or unsafe, the question of whether there is a sufficient public interest must be judged by the practitioner on the facts of each case. **Therefore, where you have a concern about a child or young person, you should consider sharing confidential information irrespective of whether you have consent to do so, if you consider the child or young person will be placed at harm if the information is not shared.**

A public interest can arise in a wide range of circumstances, for example, to protect children from significant harm, protect adults from serious harm, promote the welfare of children or prevent crime and disorder. There are also public interests, which in some circumstances may weigh against sharing, including the public interest in maintaining public confidence in the confidentiality of certain services.

The key factors in deciding whether or not to share confidential information are **necessity and proportionality**, i.e. whether the proposed sharing is likely to make an effective contribution to preventing the risk and whether the public interest in sharing information overrides the interest in maintaining confidentiality. In making the decision you must weigh up what might happen if the information is shared against what might happen if it is not and make a decision based on professional judgement. The nature of the information to be shared is a factor in this decision making, particularly if it is sensitive information where the implications of sharing may be especially significant for the individual or for their relationship with the practitioner and the service.

Taken from: [DCSF Information Sharing: Guidance for Practitioners and Managers page 21 \(HM Government, 2008\)](#)

5. Partner agencies covered by this protocol

Partners covered by this protocol are constituent partners of the WSCB and the Children's Trust, and are listed in the table below:

Worcestershire County Council – Children's Services
Worcestershire County Council – Adult & Community Services
Worcestershire Primary Care Trust
West Mercia Constabulary
Worcestershire Association of Governors
Learning and Skills Council
Worcestershire and Herefordshire Youth Offending Service

Herefordshire and Worcestershire Connexions Service
Probation Service
Voluntary and Community Sector
District Councils
Special Schools
Secondary Schools
Middle Schools
Primary Schools
GPs
Worcestershire Mental Health Partnership NHS Trust
Job Centre Plus
Worcestershire Acute NHS Trust
NSPCC
West Midlands Ambulance NHS Trust
West Mercia Probation Trust
CAFCASS
Colleges

6. Relationship of this Protocol to other Protocols

The most commonly recognised Information Sharing Protocol model consists of three tiers:

Tier 1 – At the highest level, all agencies agree a common set of principles under which they will share information with each other. This agreement, or overarching protocol, commits those who sign it to sharing information lawfully and effectively at all levels of their organisation.

Tier 2 – The middle tier begins to define a greater level of detail, with a focus on the purposes underlying the sharing of specific sets of information.

Tier 3 – This consists of detailed, specific information sharing agreements between the individual agencies. They will identify the routes through which requests for information may be made, the methods of auditing who has had access to what and the details of the information to be shared.¹

Note on language:

It is important to note that the ‘tier system’ referred to in this protocol does not relate to the four tiers of need (the pyramid) used in Children’s Services.

This Tier 2 protocol sits within an information sharing framework for Worcestershire, as agreed by the Worcestershire Partnership. The Worcestershire Partnership brings together local government, public services such as health, learning providers, police and probation, voluntary and community organisations and local businesses within Worcestershire. Their purpose is to tackle the issues that affect Worcestershire residents’ quality of life - such as crime, health, jobs, education and transport. These issues are connected and the Worcestershire Partnership believes that they can be better addressed by working together, sharing ideas and pooling resources.

The 'Worcestershire Standard for Sharing Personal Data' is a commitment by partner agencies to use a common approach to sharing personal data, based on the Data Protection Act 1998. The

¹ Definitions of 3 tier Information Sharing Protocol model derived from www.allwalesunit.gov.uk

Tier 1 protocol consists of 8 key principles, a toolkit for producing Tier 2 and 3 protocols and a web-based protocol register along with templates and reference documents.

This document's relationship to other protocols can be seen in the following table (please note that this list is not exhaustive):

Tier 1	Worcestershire Standard for Sharing Personal Data
Tier 2	<ul style="list-style-type: none"> • Protocol for sharing information between Children's Trust agencies working for children and young people in Worcestershire • General Protocol for Information Sharing across Worcestershire Acute Hospitals Trust, Worcestershire Mental Health Partnership NHS Trust, Worcestershire PCT and Worcestershire Adult Social Care
Tier 3	<ul style="list-style-type: none"> • Substance Misuse Action Team (SMAT) protocol • Children Missing from Care • Integrated Working Programme (Common Assessment Framework) • MARAC • Information Sharing Protocol for Community Safety • Wyre Forest Community Safety Partnership Joint Protocol for the Sharing of Information • West Mercia Prolific and Other Priority Offenders Operational Information Sharing Protocol • Information Exchange Protocol (The Exchange and Management of Information) • Police/Housing/Wychavon Liaison Group Meeting • Information Sharing Agreement between Worcestershire County Council and West Mercia Constabulary • Worcestershire Joined Up Information System Partnership – Information Sharing Protocol • Information Sharing Agreement between Worcester Community Housing, Rooftop Housing Group, and West Mercia Constabulary • Information Sharing Protocol for Substance Misuse Treatment Agencies • Information Sharing Protocol to facilitate Drug Interventions Programme

7. Legal basis for information sharing under this protocol

If there is no consent from the data subject, the following must be adhered to in order to share information:

1. Data Protection Act 1998 – to share information, you must meet a condition in [schedule 2](#) of the Act, or if the information is [sensitive](#), a condition in [schedule 3](#) of the Act.
2. You must identify a [legal power](#) for sharing – there are basic powers, and then more specific ones which allow or require the sharing of information.

3. Is the use of information restricted by law e.g. Child Support Act 1991 or Abortion Act 1997?
4. Does the data sharing meet the requirements of the [Human Rights Act 1998](#)?
5. Does the sharing fall into one of the [reasons](#) agreed for the purposes of this protocol?

The signatories to this Protocol are able to share information under a number of legal powers, including the Children Act 2004 and the Education Act 2002, amongst others. A full list of legal powers, along with the associated detail can be found in Appendix 2.

When sharing information, the partner agencies will work within the requirements of the national legal framework. Key elements in this are:

The Human Rights Act 2000
The Common Law duty of confidentiality
The Data Protection Act 1998
Caldicott Principles
Freedom of Information Act 2000

The principal elements of this legislation are described in Appendix 3.

For copies of the Acts go to www.opsi.gov.uk but bear in mind that amendments made subsequent to the act will not show up on these copies.

8. Reasons for sharing information

Reasons for sharing personal information under this protocol will be limited to one or more of the following:

- delivery of effective services for children, young people and their families
- safeguarding vulnerable children and young people
- assuring and improving the quality of services
- risk management
- to avoid duplication of information gathering
- to map information required for monitoring, creating or updating the Children and Young People's Plan, the Joint Strategic Needs Assessment, or any statutory return required by law.

Reasons for sharing non-personal information under this protocol will be limited to one or more of the following:

- managing and planning services
- business planning
- contracting and commissioning the provision of services
- performance management
- statistical analysis
- data cleansing exercises
- research

9. Processes for sharing information

9.1 General

All information shared under this Protocol must be accurate, current and should not be shared indefinitely. The quantity and coverage of data shared should be directly related to the purposes of sharing, and not excessive.

It is important that those individuals wishing to share information make the distinction about who 'owns' the data that is being shared. For example, employees (data controllers) within Children's Services may be maintaining a database with personal information about service users (data subjects). However they do not own that data and should not (in most cases) share it without consent from the data subject.

Data Controller – determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Subject – a living individual to whom personal data relates.

9.2 Informing individuals about the use of their data

When an agency first collects information from an individual it must comply with the Data Protection Act 1998. The agency is required to provide a Fair Processing Notice to that person who provides the following information:

- the identity of the agency who will act as the Data Controller;
- the purposes for which the agency will be processing the person's information;
- details of how and why that information may be shared with other agencies.

Agencies will establish processes to seek explicit consent to share information and will ensure that proper systems are in place to record whether consent has been given or not.

Where an agency has decided to start sharing information with an agency not noted in the Fair Processing Notice, revised Fair Processing Notices must be issued to include the new agency or agencies.

This Protocol will be a public document and will be included in the Publication Schemes of the partners, as required under the Freedom of Information Act 2000.

9.3 Confidentiality

Personal information held by an agency shall be deemed to have been provided in confidence, unless consent to share this information has been given by the subject.

All agencies accept this duty of confidentiality and will not disclose personal information without the explicit consent of the person concerned, unless there are statutory grounds or other overriding justification for doing so.

People requesting disclosure of personal information from agencies party to this Protocol will respect this responsibility and will not seek to override the procedures which each agency has in place to ensure that information is not disclosed illegally or inappropriately.

9.4 Consent

Effective and lawful information sharing is essential for early intervention to ensure the welfare and safety of children and young people. None of the current legislation, including the Data Protection Act 1998 and the Human Rights Act 1998, prevents the lawful sharing of information where this is necessary to protect children, young people and vulnerable adults.

The basic position is that consent to share information should be sought as the first option. This is best achieved by explaining to the child and young person and their family at the outset what and how information will, or could be shared, and why. However, where consent cannot be obtained or is refused, information may still lawfully be shared in order to protect a child from significant harm or adult from serious harm, or to ensure that a serious crime is prevented, detected, investigated or prosecuted. Therefore, if you have a concern about the safety of a child or young person, do not allow the refusal of consent to prevent you from sharing that information (N.B. If you do this, you should seek to advise the child/young person and their family that you have shared their information as soon as it is safe and legal to do so).

In seeking consent to disclose personal information to another agency party to this Protocol, an individual will be made fully aware of:

- The nature of the information that will be shared
- Who the information will be shared with
- The purposes for which the information will be used
- Other relevant details including their right to withhold or withdraw consent
- The potential consequences of not sharing information (e.g. this service may not be available to you).

All children and young people have the right to know how information about them will be treated and shared. It is expected that practitioners will talk through this right with every child or young person so that the child or young person understands how information will be used. Consent should be obtained from a parent or other person with parental responsibility for all children and young people under the age of 16 years.

Any young person aged 16 years or over has the right to give or withhold consent, independent of their parents' views. Any young person under 16 years of age may wish to give or withhold consent to the sharing of information, independent of and in contradiction of their parents' views. This wish should be acceded to where the young person is deemed to be of sufficient age and understanding to give informed consent. It is for the practitioner working with the young person to make that judgement, applying the Fraser guidelines (Gillick Competence).

The Fraser guidelines (Gillick Competence) are used to consider the ability of children and young people under the age of 16 to give informed consent. For young people under the age of 16, they can give valid consent if they have sufficient understanding and intelligence to appreciate fully what is proposed, and they are capable of expressing their own wishes. If a young person meets this test, their consent overrides that of the person with parental responsibility for them.

Consent must also specify with which agencies information can be shared; it cannot be assumed that a person is willing to share information simply because they have not stated to the contrary. It should be noted that, if agency A obtained consent to share information with agencies B, C and D, it does not follow that agency B has permission to share information with A, C and D. Agency B requires further consent to share information that only it has and which has not been obtained from Agency A under the consent provided originally.

Consent to disclose personal information will be limited to the duration of a 'piece of work' (specific involvement with any particular agency until case closure) the purpose for which consent was obtained. All agencies agree that once the 'piece of work' for which consent was obtained has been completed or purpose for which consent was obtained is over that consent will be deemed to have lapsed. In the event that similar or subsequent additional work needs to be undertaken with that individual, a new consent to disclose must be obtained.

Further information on consent:

[CAF Practitioner Toolkit \(CYPSP, 2007\), section 9](#)

9.5 Quality of information

All agencies are responsible for ensuring that they have processes and procedures in place for ensuring that information is recorded accurately, that there are methods in place for checking this and to ensure that shared information is of sufficient quality.

Where appropriate, 'health warnings' should be attached to the information or data which inform other agencies of any issues with the data e.g. reliability, timeliness, cohort size.

The importance of high quality data can not be underestimated. Data needs to be maintained and kept up-to-date and accurate to ensure that service planning and management decisions can be made based on sound information.

10. Security arrangements

All personal information must be kept in a secure environment, where access is controlled and security measures are in place. All agencies will put in place policies and procedures governing the security, storage, retention and destruction of personal information.

All agencies will put in place policies and procedures governing 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.

All agencies will put in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

- internal and external postal arrangements;
- verbal, face-to-face, telephone;
- facsimiles;
- electronic mail (secure network or encryption);
- electronic work transfer (must be encrypted)

All agencies will have in place appropriate measures to investigate and deal with inappropriate or unauthorised access to, or use of, personal information, whether intentional or inadvertent.

Agencies have responsibilities to ensure employees have valid e-CRB checks where appropriate. Practitioners wishing to have access to ContactPoint (launched in Worcestershire in Autumn 2009), will need to hold an up-to-date e-CRB check as one of several pre-requisites before access to the system and system training will be granted.

In the event that personal information which has been shared under the Protocol is inappropriately released or accessed, the agency making the discovery will without delay:

- inform the information provider of the details
- take steps to investigate the cause
- if appropriate, take disciplinary action against the person(s) responsible
- take appropriate steps to avoid a repetition.

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

- notify the individual concerned
- advise the individual of their rights
- provide the individual with appropriate support.
- undertake a generalised risk assessment and consider notifying the Information Commissioner's Office.

11. Processes for informing and guiding staff about the arrangements

All agencies will ensure that their staff (full/part time, members, temporary, agency, students, volunteers etc) who have access to, or are likely to come into contact with, personal information sign a confidentiality agreement as part of their terms and conditions of employment.

Agencies will ensure that all staff are aware of and comply with their responsibilities and obligations with regards to data protection. This includes:

- the commitment of the agency to only share information legally and within the terms of the Protocol;
- an understanding that information will be shared on a need-to-know basis;
- making staff aware that disclosure of personal information that cannot be justified, whether inadvertent or intentional, will be subject to disciplinary action.

Agencies will ensure that employees who need to share personal information are given appropriate training to enable them to share information legally, and comply with any professional codes of practice and any local policies and procedures.

Agencies will nominate a lead person who will be responsible for the day-to-day management of the scheme within their agency, providing guidance for staff and for ensuring that any Tier Three protocols are approved through the appropriate information governance arrangements in their agency. The person nominated will have sufficient seniority within the agency to influence policies and procedures at executive level.

Appendix 1

Signatories of this Information Sharing Protocol

This Protocol applies from 1 April 2010 and shall be reviewed annually thereafter. The Review shall be undertaken by a representative from each Partner and Data Protection Officers / Caldicott Guardians as appropriate. Partners to this Protocol are:

Organisation / Agency	Name and Job Title
Worcestershire County Council – Children's Services	Marcus Hart – Lead Member for Children and Young People / Chair of Children's Trust
Worcestershire County Council – Children's Services	Gail Quinton – Director of Children's Services
NHS Worcestershire	Sandra Rote – Director of Clinical Development and Executive Lead Nurse
West Mercia Probation Trust	Helen Allen – Head of Probation Services
Worcestershire and Herefordshire Youth Offending Service	Keith Barham – Head of Offending Service
West Mercia Police	Jane Horwood – Chief Officer for 'C' Division West Mercia (South Worcestershire)
Worcestershire Acute Hospitals NHS Trust	Helen Blanchard – Director of Nursing and Midwifery
Worcestershire Mental Health Partnership NHS Trust	Susan Fairlie – Director of Service Development and Executive Nurse
NSPCC	Liz Morris – Assistant Director NSPCC
CAFCASS	Liz Elgar – Head of Service
West Midlands Ambulance NHS Trust	Gill Bennett – Director of Nursing and Primary Care
Malvern Hills District Council	Lee Robson – Head of Community and Economic Development
Worcester City Council	Pete Sugg – Acting Head of Safer and Stronger Communities
Wychavon District Council	Ian Marshall – Head of Legal and Support Services
Bromsgrove District Council	Angie Heighway – Head of Community Services
Redditch Borough Council	Angie Heighway – Head of Community Services
Wyre Forest District Council	Linda Collis – Director of Community and Partnership Services

Original signatures will not be published within this document.

Appendix 2

Table of Legal Powers under which signatories are able to share information

Legal Power	Detail
<p><i>Children Act 2004, s10</i></p>	<p>Duty to co-operate Duty on each children’s services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:</p> <ul style="list-style-type: none"> • Physical and mental health, and emotional well-being; • Protection from harm and neglect; • Education, training and recreation; • Making a positive contribution to society; • Social and economic well-being. <p>Partners must co-operate with the local authority to make arrangements to improve the well-being of children. The relevant partners are:</p> <ul style="list-style-type: none"> • district councils; • the police; • the Probation Service; • Youth Offending Service • strategic health authorities • PCTs; • Connexions; • the Learning and Skills Council. <p>The section 10 guidance states that good information sharing is key to successful collaborative working and under this section agencies should have arrangements in place to ensure information is shared for strategic planning purposes and to support effective service delivery.</p>
<p><i>Children Act 2004, s11</i></p>	<p>Duty on key persons and bodies to make arrangements to ensure their functions are discharged with regard to the need to safeguard and promote the welfare of children. The key people and bodies are:</p> <ul style="list-style-type: none"> • local authorities (including district councils); • the police; • the Probation Service; • bodies within the National Health Service (NHS); • Connexions; • Youth Offending Service • governors/directors of prisons and young offender institutions; • directors of secure training centres; • the British Transport Police. <p>Agencies should:</p> <ul style="list-style-type: none"> • carry out their existing functions in a way that takes into account the need to safeguard and promote the welfare of children and • ensure services they contract out to others are provided having regard to the need to safeguard and promote the welfare of children. <p>In order to safeguard and promote the welfare of children, arrangements should ensure that:</p>

Legal Power	Detail
	<ul style="list-style-type: none"> • all staff in contact with children understand what to do and are aware of the most effective ways of sharing information if they believe a child and family may require targeted or specialist services in order to achieve their optimal outcomes; • all staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including those children suffering or at risk of significant harm.
<i>Children Act 1989, s47</i>	<p>Section 47 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that unless in all the circumstances it would be unreasonable for them to do so, the following authorities must assist with these enquiries:</p> <ul style="list-style-type: none"> • any local authority; • any local education authority; • any housing authority; • any health authority; • any person authorised by the Secretary of State.
<i>Children Act 1989, s17</i>	<p>Local authorities can request information from any of the list (detailed under s47) where it will help to provide services for children in need, or any other functions under part 3 of the Children Act 1989.</p>
<i>Education Act 2002, s175</i>	<p>Duty on maintained schools, further education institutions and independent schools to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children and follow the guidance in Safeguarding Children in Education (DfES 2004)</p>
<i>Education Act 2002, s21 (as amended by Education and Inspections Act 2006 s38)</i>	<p>Duty on the governing body of a maintained school to promote the well-being of pupils at the school, having regard to the Children and Young People's Plan in the local area (click here to access Worcestershire's Children and Young People's Plan)</p>
<i>Education Act 1996, s13</i>	<p>The LEA shall contribute towards the spiritual, moral, mental and physical development of the community, by securing that efficient primary and secondary education is available to meet the needs of the population of the area. Details of the number of children in the local authority's area and an analysis of their needs are required in order to fulfil this duty.</p>
<i>Learning and Skills Act 2000, s117</i>	<p>Enabling young people to take part in further education or training</p>

Legal Power	Detail
<i>Learning and Skills Act 2000, s119</i>	Enables Connexions Services to share information with Jobcentre Plus to support young people to obtain appropriate benefits under the Social Security Contributions and Benefits Act 1992 and Social Security Administration Act 1992.
<i>Education (SEN) Regulations 2001 Regulation 6</i>	When the LEA is considering making an assessment of a child's special educational needs, it is obliged to send copies of the notice to social services, health authorities and the head teacher of the school (if any) asking for relevant information.
<i>Education (SEN) Regulations 2001 Regulation 18</i>	All schools must provide Connexions Services with information regarding all Year 10 children who have a statement of special educational needs.
<i>Children Leaving Care Act 2000</i>	The local authority is under a duty to assess and meet the care and support needs of eligible and relevant children and young people and to assist former relevant children , in particular in respect of their employment, education and training. Sharing information with other agencies will enable the local authority to fulfil the statutory duty to provide after care services to young people leaving public care.
<i>Mental Capacity Act 2005</i>	Mental capacity to consent <ol style="list-style-type: none"> 1. A person must be assumed to have capacity unless it is established that they lack capacity. 2. A person is not to be treated as unable to make a decision unless all practicable steps to help him to do so have been taken without success. 3. A person is not to be treated as unable to make a decision merely because he makes an unwise decision. 4. An act carried out or a decision made, under this Act for or on behalf of a person who lacks capacity, must be done in his best interests. 5. Before the act is done, or the decision is made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive on the person's rights and freedom of action. <p>Chapter 4 of the Mental Capacity Act 2005 Code of Practice provides guidance on how to assess whether someone has the capacity to make a decision.</p>
<i>Immigration and Asylum Act 1999, s20</i>	Information sharing to enable the Secretary of State: <ul style="list-style-type: none"> • to undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act; • to undertake the provision of support for asylum seekers and their dependents.
<i>Local Government Act 2000 s2</i>	Enables local authorities to do anything to promote social, economic or social well-being in their area provided this is not specifically forbidden by another statute.
<i>Criminal Justice Act 2003, s325</i>	The following agencies must co-operate with establishing arrangements for the purpose of assessing and managing the risks posed by various offenders (including violent or sexual offenders, or those who could cause harm to the public):

Legal Power	Detail
	<ul style="list-style-type: none"> a) Youth Offending Service b) the Ministers of the Crown, exercising functions in relation to social security, child support, war pensions, employment and training c) LEA d) local housing authority or social services authority e) registered social landlord who provides or manages residential accommodation f) NHS trust, health authority, strategic health authority, PCT, local health board i) every person who is designated by the Secretary of State as a provider of electronic monitoring services
<i>Crime and Disorder Act 1998, s17</i>	Duty on local authorities, and police authorities to do all they can to reasonably prevent crime and disorder in their area.
<i>Crime and Disorder Act 1998, s37</i>	Everyone carrying out youth justice functions must have regard to the aim of the youth justice system to prevent offending by children and young people.
<i>Crime and Disorder Act 1998, s115</i>	Section 115 sets out the power (but not obligation) of any organisation to share information with the police authorities, local authority (including parish and community councils), Probation Service and health authority (or anyone acting on their behalf) for the purposes of the CDA1998. This ensures that information may be shared for a range of purposes covered by the Act, for example for the functions of the crime and disorder reduction partnerships and Youth Offending Teams, the compilation of reports on parenting orders, anti-social behaviour orders, sex offender orders and drug testing orders.
<i>Adoption and Children Act 2002, and associated Regulations</i>	Provision for obtaining, recording and keeping confidential information about adopted children and/or their relatives. The Act and Regulations, give limited express power to share information, in prescribed circumstances as laid out in the legislation. Information about pre-2002 Act adoptions remains governed by the provisions of the Adoption Agencies Regulations 1983. Legal advice should be sought before any disclosure from adoption records.
<i>National Health Service Act 2006, s82</i>	Duty on NHS bodies and local authorities to co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.
<i>NHS Confidentiality Code of Practice 2003</i>	The NHS Confidentiality Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their health records
<i>Local Government Act 1972 s111</i>	Enables local authorities to do anything conducive or incidental to the discharge of any of their functions, providing there is specific statutory authority to carry out those functions.

Appendix 3

Guidance on issues around the legal framework of information sharing

(Based on HM Government ECM documentation)

The main legal framework relating to the protection of personal information is set out in:

- The Human Rights Act 1998 (including the right to a private and family life)
- The common law duty of confidentiality
- The Data Protection Act 1998 (covering protection of personal information)

There is no general statutory power to share information, just as there is no general power to obtain, hold or process data. Some Acts of Parliament give public bodies express statutory powers to share information.

Where there is no express statutory power to share information it may still be possible to imply such a power from the other duties and powers public bodies have. Many activities of statutory bodies will be carried out as a result of implied statutory powers, particularly as it may be difficult to expressly define all the numerous activities that a public body may carry out to deliver its main duties and powers.

Having express or implied statutory powers in any particular case does not mean that the Human Rights Act 1998, the common law duty of confidentiality, and the Data Protection Act 1998 can be disregarded. Where a statutory provision explicitly removes the need to consider confidentiality, then confidential information can be shared however this will be rare and in limited circumstances. Where there are implied powers you need to consider the language of the provision and the surrounding circumstances.

There is also a brief overview of the Caldicott Principles.

Human Rights Act 1998

The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable action within their powers (which would include information sharing) to safeguard the Convention rights of individuals. These rights include the right to life (Article 2), the right not to be subjected to torture or inhuman or degrading treatment (Article 3) and the right to liberty and security (Article 5).

Article 8 of the European Convention on Human Rights was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect private and family life, home and correspondence. Sharing confidential information may be a breach of an individual's Article 8 right: the question is whether sharing information would be justified under Article 8.2 and proportionate.

The right to a private life can be legitimately interfered with where it is in accordance with the law and is necessary, for example,

- for the prevention of crime or disorder,
- for public safety,
- for the protection of health or morals, or
- for the protection of the rights and freedoms of others.

You need to consider the pressing social need and whether sharing the information is a proportionate response to this need and whether these considerations can override the individual's right to privacy. If a child or young person is at risk of significant harm, or an adult is at risk of serious harm, or sharing is necessary to prevent crime or disorder, interference with the individual's right may be justified under Article 8.

Common Law Duty of Confidentiality

The common law provides that where there is a **confidential relationship**, the person receiving the **confidential information** is under a duty not to pass on the information to a third party. However this duty is not absolute and information can be shared without breaching the common law duty if:

- the information is not confidential in nature; or
- the person to whom the duty is owed has given explicit consent; or
- there is an overriding public interest in disclosure; or
- sharing is required by a court order or other legal obligation
- it is to prevent serious crime and/or maintain national security
- it is to prevent serious harm or abuse.

Confidential information is

- personal information of a private or **sensitive nature** (see below)
- information which is not already in the public domain
- information which has been shared, but the person giving the information would reasonably expect that it would not be shared with others

A **confidential relationship** can be

- formal – e.g. social worker and client, nurse/doctor and patient
- informal – e.g. pupil and teacher, where the conversation was informal and the pupil only asks the teacher to keep some of the information confidential.

Sensitive personal data is personal data relating to racial or ethnic origin, religious or other similar beliefs, physical or mental health condition, sexual life, political opinions, membership of a trade union, the commission or alleged commission of any offence, any proceedings for an offence committed or alleged to have been committed, the disposal of proceedings or the sentence of any court in proceedings.

Data Protection Act 1998

The Data Protection Act 1998 (DPA) deals with the processing of personal data. Personal data is data which relates to a living person, including the expression of any opinion or indication about the intentions in respect of the individual. Sensitive personal data is personal data relating to racial or ethnic origin, religious or other similar beliefs, physical or mental health condition, sexual life, political opinions, membership of a trade union, the commission or alleged commission of any offence, any proceedings for an offence committed or alleged to have been committed, the disposal of proceedings or the sentence of any court in proceedings.

Information about an individual will often contain information from several sources, for example from schools, doctors or the police and may contain their names and business addresses. It may also include information about other people, for example the individual's family members. These people are usually referred to in the DPA as 'third parties'. Information about third parties is personal information and should be treated accordingly.

If an individual is no longer alive their personal information is not covered by the DPA although a duty of confidence may require some or all of their personal information to be kept confidential.

Organisations which process personal data must comply with the data protection principles set out in the DPA. These require data to be:

1. *fairly and lawfully processed, in particular it shall not be processed unless a schedule 2 condition is met, and if sensitive personal data, a schedule 3 condition is also met;*
2. *processed for limited specified purposes;*
3. *adequate, relevant and not excessive for those purposes;*
4. *accurate and up-to-date;*
5. *kept for no longer than necessary;*
6. *processed in accordance with the data subject's rights under the DPA;*
7. *kept secure;*
8. *not transferred to non-EEA (European Economic Areas) without adequate protection.*

What do the 8 DPA Principles mean in practice?

1. *fairly and lawfully processed, in particular it shall not be processed unless a schedule 2 condition is met, and if sensitive personal data, a schedule 3 condition is also met;*

The first principle introduces the requirement that personal data shall not be processed unless at least one of the conditions in Schedule 2 of the Act is met and, in the case of processing sensitive personal data at least one of the conditions in Schedule 3 of the Act is also met. Meeting a Schedule 2 and Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful. The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

Schedule 2 conditions include:

- the data subject has given consent to the data processing
- the processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to entering into a contract
- the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract
- the processing is necessary to protect the data subject's vital interests
- the processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, 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 or a government department, for the exercise of any other public functions exercised in the public interest by any person
- the processing is necessary for the purposes of legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, except where the processing is unwarranted by reason of the rights and freedoms or interests of the data subject

When information is sensitive then a schedule 3 condition must also be met. These are:

- the data subject has given explicit consent to the processing
- the processing is necessary for the purposes of exercising any legal right or obligation on the data controller in connection with employment
- the processing is necessary to protect the vital interests of the data subject or someone else, in a case where the data subject cannot give consent or consent cannot reasonably be obtained, or, in order to protect another person's vital interests, the data subject is unreasonably withholding consent
- the processing is carried out by a not-for-profit body in the course of its legitimate activities and does not involve disclosure of the personal data to a third party without consent
- the information has been made public as a result of steps taken by the data subject
- the processing is necessary for the purposes of, or in connection with any legal proceedings, obtaining legal advice or to establish, exercise or defend legal rights
- the processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, for the exercise of any functions conferred on any person by or under any enactment, or for

- the exercise of any functions of the Crown, a Minister or a government department
- the processing is necessary for medical purposes and is undertaken by a health professional
- the processing is of sensitive personal data consisting of information as to racial or ethnic origin and is necessary for the purpose of promoting racial or ethnic equality and is carried out with appropriate safeguards.

2. processed for limited specified purposes:

The second principle is that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed further in any manner incompatible with that purpose or those purposes. The interpretation of the second principle also provides that in deciding whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained; consideration will be given to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

3. adequate, relevant and not excessive for those purposes:

The third principle is that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. In complying with this principle, data controllers should seek to identify the minimum amount of information required in order to properly fulfil their purpose. This will be a question of fact in each case. For example, you do not have to share a whole case file – you could just share part of it.

4. accurate and up to date:

The fourth principle is personal data shall be accurate and, where necessary, kept up-to-date. The fourth principle is not to be taken as being contravened because of any inaccuracy in personal data which correctly records information obtained by the data controller from the data subject or a third party in a case where:-

- (a) reasonable steps have been taken to ensure the accuracy of the data
- (b) if the data subject has notified the data controller of their view that the data is inaccurate, the data indicates this fact.

5. kept for no longer than necessary:

The fifth principle is personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The DPA stipulates that records should be kept no longer than is necessary for the purposes for which the records are being processed. There are no actual timescales imposed. It is a matter for individual judgement, taking account of the nature and purpose of the records. It is advisable for all organisations to retain information on individuals to agreed timescales. Six years is a commonly used benchmark and is generally compatible with limitation periods for the commencement of legal proceedings. However longer or shorter periods may be appropriate, depending on the circumstances.

6. processed in accordance with the data subject's rights under the DPA:

i.e. processed in accordance with the rights in the DPA, as detailed.

7. kept secure:

The seventh principle is that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In relation to front-line practices, the ICO legal guidance on the DPA provides the following illustrative examples:

In relation to controlling access to information:

- can casual passers-by read information off screens or documents?
- is printed material disposed of securely, for example, by shredding?

- is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?

In relation to staff selection and training:

- is proper weight given to the discretion and integrity of staff when they are being considered for employment, promotion or for a move to an area where they will have access to personal data?
- are the staff aware of their responsibilities? Have they been given adequate training and is their knowledge kept up to date?
- do disciplinary rules and procedures take account of the requirements of the Act? Are these rules enforced?

8. not transferred to non-EEA (European Economic Areas) without adequate protection.

Caldicott Principles

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:-

- Justify the purpose(s) for using personal information
- Only use personal information when absolutely necessary
- Use the minimum amount of personal information that is required
- Access to personal information should be on a strict need-to-know basis
- Everyone with access to personal information must be aware of his/her responsibilities
- Everyone with access to personal information must understand and comply with legislation that governs personal information.

All NHS and Social Care organisations should have a Caldicott Guardian identified to ensure compliance with these principles.

Within Worcestershire, any issues regarding Caldicott Principles should be directed to:

Worcestershire Acute NHS Trust – Medical Director

Worcestershire Primary Care Trust – Director of Clinical Development & Lead Executive Nurse

Worcestershire Mental Health Partnership NHS Trust – Director of Service Development and Executive Nurse

Adult and Community Services – Head of Business and Finance

Children's Services – Head of Commissioning and Quality

Appendix 4

Glossary of Terms

Acronym / Abbreviation	Full Description
CAF	Common Assessment Framework
CAFCASS	Children and Family Court Advisory Support Service
CDA	Crime and Disorder Act
ChS	Children's Services
CRB	Criminal Records Bureau
CYPSP	Children and Young People's Strategic Partnership (now referred to as Children's Trust)
DCS	Director of Children's Services
DCSF	Department for Children, Schools and Families
DfES	Department for Education and Skills (now referred to as DCSF)
DPA	Data Protection Act
ECM	Every Child Matters
EEA	European Economic Areas
GP	General Practitioner
HM Government	Her Majesty's Government
ICO	Information Commissioners Office
JCB	Joint Commissioning Board
LEA	Local Education Authority (now referred to as Local Authority)
MARAC	Multi-Agency Risk Assessment Conferences
NHS	National Health Service
NSPCC	National Society for the Prevention of Cruelty to Children
PAB	Professional Advisory Body
PCT	Primary Care Trust
Q&P	Quality and Performance
SDM	Service Development Manager
SLT	Senior Leadership Team
SMAT	Substance Misuse Action Team (now referred to as DAAT – Drug and Alcohol Action Team)
WCC	Worcestershire County Council
WSCB	Worcestershire Safeguarding Children Board