

Toolkit for developing information sharing protocols.

Introduction

The national agenda for public services improvement requires effective co-operation between organisations to meet the needs of the public. Sharing personal data is a key element of this agenda, to protect vulnerable children and adults, and to deliver efficient services to the wider public.

Whenever personal data is collected and shared, the rights and freedoms of individuals must be respected. The Data Protection Act (DPA 1998) ensures that we *can* share personal data, without compromising the rights of individuals. The Government recommends the creation of Information Sharing Protocols, to set a clearly defined framework within which personal data can be shared fairly & lawfully.

This toolkit is part of the Standard for Sharing Personal Data which is a robust framework for the legal, secure and appropriate sharing of personal data between public sector agencies in Worcestershire. The Standard is based on the Data Protection Act and is consistent with national best practice. The purpose of the Standard is to:

- Develop understanding of data protection boundaries.
- Co-ordinate the development of protocols across agencies, reducing duplication.
- Clarify roles and responsibilities with regard to information sharing.
- Encourage training and support on information sharing at an operational level.
- Share best practice and raise the quality of information sharing agreements.

Information Sharing Protocols

This toolkit sets out a series of steps to create an information sharing protocol, based on the requirements of the Data Protection Act 1998. Information Sharing Protocols are agreements between organisations (or sometimes between distinct parts of one organisation) wishing to share personal data for practical and specific purposes. The agreement confirms what data is to be shared, what the purpose of sharing is, and what the restrictions on the uses of that information are. Responsibilities are agreed and the protocol is to be signed by each Partner involved. Information Sharing Protocols help to understand the legal requirements to share information, where consent is required, and where information cannot be shared.

The Standard has been developed based on real projects creating protocols, and examples of these are used within the toolkit.

- | | | |
|--|---|---|
| S
t
e
p
s | 1 | Agreeing the purpose |
| | 2 | Establishing ownership and responsibility |
| | 3 | Planning the sharing, and understanding the law |
| | 4 | When using consent |
| | 5 | Retaining information and security |
| | 6 | Communicating with individuals |
| | 7 | Approval, implementation and review |

step

1

Agreeing the Purpose of Sharing Information

- 1.1 Agencies which need to share information for a specific purpose may find that
 - Practitioners are uncertain about their responsibility and the legal boundaries,
 - Different agencies apply different approaches to sharing information,
 - Information sharing is inconsistent and ineffective

Creating a formal information sharing agreement or protocol can help to ensure consistency and remove any uncertainty and conflict.
- 1.2 The agencies which want to create a protocol should nominate representatives to form a **Protocol Working Group**. Their first task is to be clear about whether a protocol is needed, and for what purpose.
- 1.3 At the earliest point it is important to talk to your '**Data Sharing Standard lead officer**'. Each Partner who has signed up to the Worcestershire Standard for Sharing Personal Data has one. They will be able to advise on whether there is an existing agreement that applies, or could be adapted. The role of the lead officers is to:
 - Keep a record of any protocol development that involves their organisation;
 - Promote the Standard and guide people on its use;
 - Advise on who to involve in the protocol & how to get the business case agreed.
- 1.4 If a new protocol is required, the Protocol Working Group may need to develop the initial business case, explaining why the protocol is needed. This business case (see [Template 1](#)) is used to gain a mandate from senior managers. The purpose of the protocol must focus on the better outcome achieved by sharing information, for example sharing information to support elderly victims of crime, or enabling early intervention where children are vulnerable. See [Example 1](#). If the purpose relates to children and young people the cross Government Guidance 'Sharing Information on Children and Young People' will be helpful for reference.
- 1.5 There are two types of information sharing protocols which the Working Group may choose to develop, depending on the scope of the purpose:
 - A general agreement which gives boundaries to the creation of more specific protocols but doesn't go into specific detail (known as **Tier 2 Protocols**).
 - A specific agreement which details who passes what information to whom, when, and under what circumstances (known as **Tier 3 Protocols**) - these agreements are specific & practical, often including flowcharts or process maps.

Tier 2 protocols are useful to prepare for subsequent Tier 3 protocols, saving time and ensuring consistency by defining the general rules which apply to information shared within a defined community. For example, Children's Services partners, including health, education, social care, Connexions, Youth Offending Service, Police, & District Councils will need to share information at many different points to provide services for families effectively, so may need a number of specific (Tier 3) agreements to support sharing where the processes differ. The context for these could be set by a general (Tier 2) agreement, defining principles, ethics, terminology, professional practice, local variation, training, communication, ownership and so on. ([See Protocol Templates](#))

Business case template

Name of Pilot Project

Name and contact details of Protocol Co-ordinator (see Step 2)

Purpose and Scope

- Level of the Protocol (Tier Two/Three)
- Purpose of the Protocol
- Reasons for developing a protocol
- Benefits to be gained from using a protocol
- Options considered
- Costs and timescales
- Major risks

Partners to this business plan

Agency (Specify which part of the agency if appropriate)	Lead Person (Name & job title, of person developing the protocol)	Protocol mandate (Who commissions and sign off the protocol?)
1.		
2.		

Example: Purpose

The WANDs Children's Centre has developed a protocol for sharing registration information between the agencies delivering services at the Centre for young children and their families. The protocol explains the purpose for sharing information as:

'The overarching purpose for sharing information is to provide an integrated and seamless service for children and families within our Sure Start area (Westlands & Chawson) in line with our Children's Centre remit, specifically

- *enabling early intervention where children are vulnerable to risk*
- *ensuring families are referred on to appropriate services to cater for their needs'*

Is a Tier 2 or 3 protocol required?

- How specific is the purpose for the information sharing agreement? Is it too wide to be covered by a single Tier 3 protocol?
- Is there already a Tier 2 Protocol? - an existing agreement which broadly covers this specific arrangement. If so, you may need to create a Tier 3 Protocol
- Are a number of other similar Tier 3 protocols likely to be needed, involving mostly the same partner agencies? If so, you may wish to produce a Tier 2 Protocol
- Would it save time in the longer-term to establish a Tier 2 protocol which can be used subsequently to develop a range of Tier 3 protocols?

step

2

Establishing Ownership and Responsibility

- 2.1 Once the business case has been prepared, ownership by the agencies that will be partners to the protocol needs to be established. The [example](#) on the opposite page describes how the WANDs Children's Centre brought partner agencies together.
- 2.2 Agreement to the business case by a **senior manager** within each of the partner agencies is the first step. They will be responsible for both commissioning and signing off the protocol so their commitment from the beginning is vital. They should be the senior staff member strategically responsible for the work that the information sharing supports. Protocols which have been methodically detailed can nonetheless fail to gain formal approval because this step was omitted.
- 2.3 Once the senior level mandate is in place the next step is to re-form the **Protocol Working Group**. Membership of this Group is likely to have grown as more partners have been persuaded by the business case. Group members should have sufficient seniority to complete the task on behalf of their agency, and also a good understanding of current practical arrangements for using information. The Group will include or liaise with Partner Data Protection Officers and Caldicott Guardians (where these exist) (see glossary).
- 2.4 The Group should nominate a **Co-ordinator** whose task is to drive forward the arrangements to develop the protocol. This person should register the protocol plans on the Standard website – www.worcestershirepartnership.org.uk/datasharing - through their Data Sharing Standard Lead Officer.
- 2.5 The Group should establish a process to engage with stakeholders, such as operational staff and the public, to ensure that the protocol is workable in practice.
- 2.6 If any of the Partners are managing information *on behalf* of another organisation (for example, where a service is contracted out), this may need a different type of information sharing agreement (see Data Protection Act 1998, Schedule 1, Para 12). This should be discussed with Partner Data Protection Officers before proceeding.
- 2.7 The initial work carried out when developing the business case can now be used to start creating a new document; the written Protocol (see [Protocol Structure](#) for full contents that are further explained during this Toolkit). Partners, purpose and scope have already been defined, and some general principles which the Data Protection Act sets can be added now to this Protocol, namely:
 - The information can only be used for the purpose for which it was collected;
 - If any of the Partners to the protocol want to change the purpose, all Partners need to agree to the change;
 - If any of the Partners to the protocol want any of the data for further statistical purposes, any personal information should be anonymised.
- 2.8 Templates for both Tier 2 and 3 protocols are given in [Appendix 2](#)

WANDs: Bringing Partners together

The WANDs Children's Centre Manager took the lead in developing a protocol covering sharing personal information between the agencies delivering services in the Centre. She started by checking out the concepts with a mentor, her organisation's Data Protection Officer and her line manager.

She then started talking to key partner agencies to build support for the approach. This included both 1:1 discussions and built up to a series of group workshops. The idea of creating a formal information sharing agreement was new to some of the partner agencies delivering through the Centre, and so much time needed to be spent on the potential benefits, explaining why a change was needed to improve arrangements. Although the approach wasn't confrontational, some partners found the discussions difficult and it took 2-3 months to build confidence. WANDs is now using Service Level Agreements with agencies to require sign up.

Tier 3 Protocol Structure

1. Name of Protocol and List of Partners involved

2. Purpose of sharing information
3. Relationship of this Protocol to other Protocols
4. Specific information which will be shared
5. Legal basis for sharing this information
6. Processes for sharing the information, defining for each piece of data:
 - Who collects it
 - Who is to receive it
 - Conditions for sharing (eg consent, legal obligation, statutory function)
 - Caveats on sharing (eg anonymised data only, or restricted only to certain named officers)
 - How long the information will be retained
7. Processes for informing individuals about use of their data
8. Processes for informing and guiding staff about the arrangements
9. Additional requirements, for example security arrangements, or notification of the Information Commissioner
10. Signatures, Date from which Protocol applies & Review date
11. Appendices, for example consent form, named officers for sharing, information sharing policy/leaflet.

step

3 Planning the sharing, and understanding the law

- 3.1 The Protocol Working Group now needs to define what specific information is to be collected and shared, how this will be done, and what is the legal basis for this.
- 3.2 Start by identifying the personal information that must or could be shared in order to meet your purpose. Examples of how to group this information into data categories are given below. The example categories given may be transferable to your protocol or you may need to define your own categories.

Example Data Categories: Vulnerable Adults Information Sharing Protocol	
Data Category	May include: (only where necessary & relevant)
Data subject – basic person details	Full Name, address, postcode, date of birth, gender, occupation, NHS no.
Data subject – sensitive person details	Racial/ethnic origin, physical and mental health or condition, sexuality, criminal offences and proceedings (including alleged). (Less likely: political opinions, religious/similar beliefs, trade union membership).
Data subject – financial details	Account details, power of attorney details, benefits, arrears, debt details
Carer Information	Names, address, date of birth, relationship to data subject
Composition of household	Names (may include maiden and other names), dates of birth, address of others in the household, relationship to data subject
Details of an allegation	Category of abuse, details of suspected abuser and of suspected abuse

- 3.3 Then map out any current processes used for collecting and sharing the personal information which you have identified as needed for the purpose: which Partners collect the data; and when they do so; which Partners then need to receive the information to meet the agreed purpose, and under what circumstances. Also record whether you carry out this sharing now, and whether information is shared in a way that meets the purpose.
- 3.4 Mapping the path that the information flows in this way will help to understand current processes and test out whether they are effective. Processes may need to be adapted to reduce duplication, avoid sharing without a legal basis, or unblock a potential information flow. It is crucial that agencies only share information which is necessary for the purpose, and do not share too much.

Clarifying the legal basis for sharing personal information

- 3.5 Now you are clear about your current sharing situation, you need to turn to the law. The circumstances under which the information can be shared are governed by the Data Protection Act, Human Rights Act, and any relevant laws to your area of work. Don't assume it's legal just because you've always done it like that. In certain circumstances the public interest in sharing confidential information overrides the public interest in maintaining confidentiality – confidentiality should not be interpreted as secrecy.

- 3.6 Firstly, the [Data Protection Act](#) (DPA 1998) gives specific boundaries to sharing personal data so as to protect the privacy of individuals. Any sharing must meet a condition in Schedule 2 of the Act, and if sharing sensitive information, you will *also* need to meet a condition in Schedule 3. See Page 9 for more on DPA conditions and ensure that at least one of these conditions is included in your Protocol.
- 3.7 Secondly, the law requires you to identify legal powers for sharing. Two pieces of legislation provide basic legal powers which can support information sharing:
- The Local Government Act, 1972, which empowers local authorities to do anything necessary to facilitate the discharge of their *statutory* functions
 - The Local Government Act 2000 enables local authorities to promote the economic, social or environmental wellbeing of a community area or its people.
- 3.8 Alternatively, you may be able to rely on another legal power that explicitly **allows** or **requires** you to share information for your purposes, for example:
- The Crime and Disorder Act, Section 115 **allows** anyone to disclose information to a police authority/local authority *if* that disclosure is necessary for the purposes of crime prevention.
 - The Children Act 1989 **requires** consideration of the need to refer to Social Services (social care) a child who is in need.
- Choosing a basic or specific power to share and stating it in the Protocol is important.
- 3.9 Thirdly, you will need to ensure that you are *not breaking* any law in sharing the information. Sometimes use of information will be specifically restricted by law. Data collected for Council tax purposes cannot be used for another purpose such as marketing (Local Government Finance Regulations 1992). Other laws such as the Child Support Act 1991 and the Abortion Act 1997 restrict the use of information because of the confidential nature of such data.
- 3.10 Fourthly, the data sharing must meet the Human Rights Act requirement that any interference by a public body with an individual be
- in accordance with the law;
 - in pursuit of a legitimate aim (for example crime protection, national economic wellbeing, protection of health/morals, public safety, protection of others rights);
 - necessary in a democratic society (is sharing necessary and fair?)
- 3.11 Once you have checked the legal bases for sharing each piece of data you may end up with a process map which looks something like this:

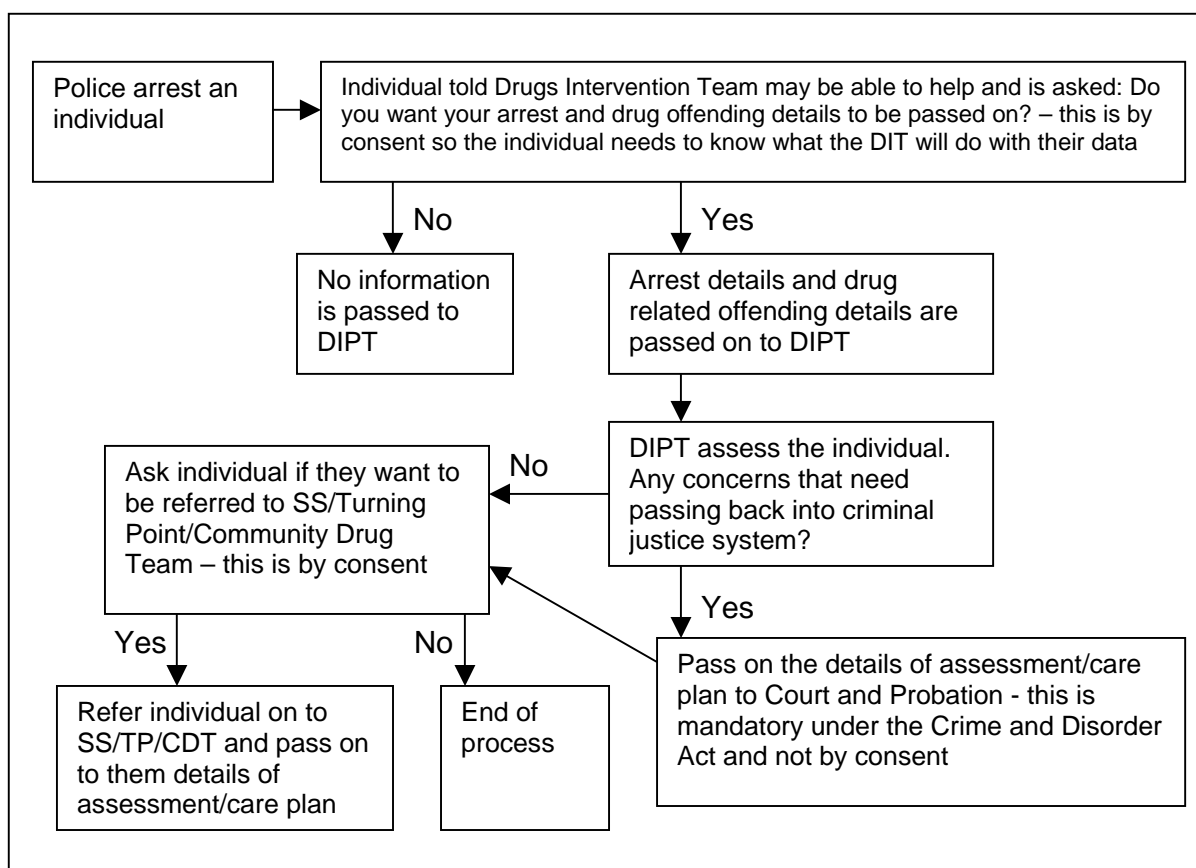
Data Category	Details of Arrest
Partner collecting	Police
When collected	At the point of arrest
Data shared with	Drugs Intervention Programme Team
How shared	
Circumstances (Data Protection condition)	When consent has been given by the person arrested

The circumstances box should indicate the Data Protection condition, or state that data will be anonymised before sharing. This can be transferred to a larger map:

Data Categories	Data held by	Data shared with	DP Condition
Details of arrest / Drug related offending	Police	DIP Team	Consent
Details of Assessment and Care plan	DIP Team	Probation service Court service Social Services Turning Point CDT	Legal* Legal* Consent Consent Consent
Details of Sentence	Court Service	Probation service Prison service DIP Team	Legal* Legal* Legal*
Details of release from prison inc early release	Prison service	DIP Team Probation	Legal* Legal*
Details of Completion of Community sentence	Probation service	DIP Team CDT Turning Point	Legal* Consent Consent
Details of leaving Treatment planned/unplanned	CDT Turning Point	DIP Team	Consent

* Legal = here, necessary for prevention/detection of crime under Crime and Disorder Act

3.12 Mapping the information path can also be helpfully presented in a flowchart:



3.13 You will need to record the results of your mapping in your protocol. This means

- Stating (in the table or flowchart) which DPA Schedule 2 condition the Protocol relies on. Your Protocol may rely on several conditions for different elements of the sharing. For example, consent may be used when transferring registration

forms between agencies, but it may be mandatory, under Child Protection law to transfer other details at certain stages.

- Stating in the Protocol which legal power you are using to share information. It may be as general as the Local Government Act 2000 or as specific as, for example, the Sale and Supply of Goods to Consumers Regulations, 2002. (NB: This is a separate requirement to meeting a condition under the DPA. There must always be a legal basis).
- Stating if there any restrictions to the sharing, because of law.

The Data Protection Act (DPA) 1998

[back to legal basis notes](#)

Processing **personal data** (in whatever format), includes obtaining, using, disclosing, sharing, destroying. Whenever Partners process, they must meet a condition in **Schedule 2** of the DPA. Schedule 2 sets out the conditions on which information can be processed – each processing operation (e.g.: each obtaining, each disclosure) must meet **one** of the following conditions:

- Consent of the data subject (the person the information relates to) has been given;
- Processing is necessary for a contract to which the data subject is party;
- Processing is necessary for compliance with legal obligation;
- Processing is necessary to protect the vital interests of the data subject (usually life or death);
- Processing is necessary for the administration of justice, for the exercise of functions conferred by enactment, for functions of a public nature exercised in the public interest;
- Processing is necessary to satisfy the legitimate interests of the Data Controller/a third party, except where this prejudices the rights and freedoms of the data subject. (This is a tricky one and should only be used with caution).

If sensitive personal data is being processed, a Schedule 3 condition must *also* be met:

- Explicit consent of data subject
- Processing is necessary for Employment Law
- Processing is necessary to protect vital interests of data subject or another, where consent cannot be given or has been unreasonably withheld
- Processing is by a not-for-profit organisation and has safeguards to protect the rights and freedoms of individuals
- Processing is of information made public by deliberate action of data subject
- Processing is necessary for legal proceedings
- Processing is necessary for the administration of justice, for the exercise of functions conferred by enactment
- Processing is necessary for medical purposes, undertaken by a health professional
- Processing is of racial/ethnic origin data and is necessary to monitor equality of opportunity
- Processing is specified by order of the Secretary of State

The Data Protection Act defines ‘sensitive’ personal data as:

- the racial/ethnic origin of the data subject
- his/her political opinions
- his/her religious or similar beliefs
- his/her membership of a trade union
- his/her physical or mental health or condition
- his/her sexual life
- the commission or alleged commission by him/her of an offence and any related proceedings

step

4

When Using Consent

- 4.1 As part of the Protocol you may choose to use consent as the condition for sharing information. Consent should only be considered where there is a genuine opportunity to decline. Partners should *not* ask for consent if they intend to go ahead with the processing anyway because of another condition.
- 4.2 There is a difference between asking for consent, and informing people what you are doing with their personal data. Informing people is explained in Step 6.
- 4.3 Gaining consent to share information requires key questions to be answered:
- Does the person giving consent have the capacity to do so? They should be able to understand and consider the issues relevant to making a decision.
 - Are they fully informed? They will need to understand why their information needs to be shared, and with whom the information may be shared.
 - Is the consent freely given?
 - Is it time limited? Consent should be considered to have lapsed after a certain point – for example once a person is no longer receiving an agreed service. This should be explicitly stated.
 - Can it be freely withdrawn or refreshed, and is the process for doing so clear and accessible to the person giving consent?
- 4.4 A young person aged 16 or 17, or a child under 16 who has the capacity to understand and make their own decisions, may give (or refuse) consent.
- 4.5 Repeated requests for consent over minor issues should be avoided by, wherever possible, gaining explicit consent for all known purposes at the earliest point.
- 4.6 If the Protocol Working Group is relying on consent for the sharing of personal data the Protocol should detail:
- How consent will be gained. Consent for sharing **sensitive** personal data should be in writing and any withdrawal of consent must be communicated to all parties involved with that individual's personal data for that purpose. Consent for sharing **non-sensitive** personal data may be collected non-verbally or orally, and be witnessed and recorded.
 - How records of consent will be maintained.
 - How individuals will be informed about giving and withdrawing consent, for example using an information leaflet which is adapted for its intended audience.
 - How staff will be informed and guided on consent.
- 4.7 Any consent form templates should be appended to the Protocol. See [Example 4](#).

Example 4 –Example of a consent form

Name

Address

If you choose to complete this form, the information you provide will be shared with X agency to provide you with an optional Support Service. Your form will be retained for only 1 year after the support has been provided.

Your details will only be accessed by those employees of the X agency who provide support.

You can withdraw your consent to this use of your information at any time but this may affect the level of support which can be provided.

You have a right to access the information we hold about you, subject to exemptions under the Data Protection Act 1998. You also have a right to complain. Please contact ***** or write to ***** for more details.

I confirm that I have understood the information above and I consent to my details being used accordingly

Signature

Date

If you are unable to manage your own affairs and someone has been appointed to sign for you then please pass this form to them to read and sign if they consent to your personal data being used as explained above.

step

5

Retaining Information and Security

- 5.1 The Data Protection Act requires that personal data is kept no longer than is necessary for the specific purpose it was collected (unless for legitimate historical purposes). It is therefore important that when data is shared, the length of time the information should be kept is agreed.
- 5.2 Each Partner should have procedures for records management. Worcestershire County Council have devised a disposal schedule (see [Example 5](#)). Some District Councils also have retention/disposal schedules. Partners should liaise, where appropriate, with those responsible for records management in their agency for information about retention periods. See [Example 6](#) for an approach to retention.
- 5.3 The Protocol Working Group should ensure that retention periods for specific activities are aligned between the Partners for the information being shared. Therefore, shared data will be kept for either the same amount of time by each Partner, or for set times as appropriate. (For example, one Partner may only need the data for 6 months, another may need it for 50 years).
- 5.4 All retention periods should be decided at the outset and communicated to those staff handling the data. Retention periods apply no matter what the format is. Electronic records also need to be retained and destroyed in the same way.
- 5.5 The Data Protection Act also requires that appropriate measures are taken to protect personal data from misuse, damage or loss. Security requirements are key to information sharing and should take account of the sensitivity of personal data.
- 5.6 Examples of security arrangements are:
 - Staff training and procedures for security of personal data, confidentiality, and data protection;
 - Password protection, physical access controls;
 - Secure means of storing & transferring personal data, manually & electronically;
 - Business continuity plans or disaster plans;
 - The security standard ISO17799. (The Department for Constitutional Affairs recommends this as the benchmark for information security).
- 5.7 Partners will need to be confident that security arrangements are adequate to safeguard personal data. Where they are not this would prevent information from being shared. A common standard of security, appropriate to the nature of the personal data, should be agreed and be explicit in the Protocol.
- 5.8 Where any Partner wished to sub-contract the processing of personal data as part of the Sharing Protocol, arrangements would need to be made to ensure that the data would only be used according to the terms of the protocol. For sub-contracting, a special agreement is needed (see Step 2.6).
- 5.9 Principle 4 of the Data Protection Act requires that personal data is accurate and, where necessary, kept up to date. Mechanisms should be in place for ensuring accuracy. The Working Group may wish to identify one Partner as responsible for checking the accuracy of personal data held, at specific intervals, and reporting inaccuracies back to Partners with whom the information has been shared.

Example 5: Worcestershire County Council Disposal Schedule, setting retention periods for certain documents:

Disposal Schedule - Microsoft Internet Explorer

Address: http://128.1.222.5:8081/sid/sts-culture-index/sts-mru-index/sts-mru-disposal-schedule-confirm.htm?Division=Education%20Welfare

Services

- MRU
- Management Strategy
- Disposal Schedule
- Transfer Sheet
- Contacts
- Information Management
- IMG
- Electronic Records
- News

Content Author:

- MRU
- Sam Ferguson
- Data Protection
- Deborah Wilson
- Electronic Records
- Heidi Lutzner

Reset Text

from the drop down list.

Function	Record Class Examples	How long does it need to be kept?	Why does it need to be kept for this long?	Then what?	Who is responsible for master copy?
Child Employment - Investigations	<ul style="list-style-type: none"> Investigation sweep check sheet employer signature sheet 	Current academic year + 3 years	Business need	Destroy	Education Welfare
Child Employment - Investigations	<ul style="list-style-type: none"> Reports of child working 	Current academic year + 3 years	Limitations Act 1980 s11	Destroy	Education Welfare
Child Employment - investigations	<ul style="list-style-type: none"> Specific investigations files signed cautions audio tapes 	Review annually and destroy non core information	Business need	Destroy 5 years from final action	Education Welfare
Child Employment - Permits	<ul style="list-style-type: none"> Application forms, permits, correspondence Employer's returns Withdrawn permits Routine visit record 	Current academic year + 3 years	Limitations Act 1980 s11	Destroy	Education Welfare
Child Employment - permits	<ul style="list-style-type: none"> Register of employers 	Until superseded	Business need	Replace	Education Welfare
Clothing grants	<ul style="list-style-type: none"> Completed application forms Standard correspondence 	Current Financial Year + 4 Years	Business need	Destroy	
Euro Key Stage 4 Project - Children	<ul style="list-style-type: none"> Child referral forms Correspondence 	Current academic	Business need	Destroy	

Example 6: Vulnerable Adults Protocol statement on retention

Appropriate retention periods shall be applied to the data to be shared to protect vulnerable adults. Each Partner should ensure these retention arrangements are fulfilled. Each Partner should ensure they have a standard retention schedule from which to work (Worcestershire County Council's schedule is developed by the Modern Records Unit; the Department of Health have produced retention guidance).

It is recommended that a master copy of Adult protection case files should be retained for 7 years from the closure of services, unless an investigation into a particular case extends this period. However, this period will need to be judged against the production of guidance on retention practice resulting from the Bichard Inquiry into the Soham murders.

step

6

Communicating with individuals

- 6.1 The Data Protection Act states that personal information must be *fairly obtained* for *specified purposes*. This means that when the data is first collected, the data subjects must be told:
- Who is collecting their information;
 - What personal details will be used for and who they will be shared with;
 - Anything else that is important to state in order to ensure they are fully informed.
- 6.2 Therefore, if personal information is being collected for one reason (e.g. to record a crime) and it is intended to use it for another (e.g. to provide victim support), then the data subjects must be told about both purposes.
- 6.3 This is a separate issue to gaining consent. You may wish to choose consent as your *condition* for sharing, but this is unconnected to the obligation to inform people *what you are doing* with their personal data.
- 6.4 Unless the purpose is obvious, or the information is given verbally, all of this information should be included in a *Fair Obtaining Notice* and given to the data subjects prior to, or at the time of, collection of their personal data. Sometimes Fair Obtaining Notices are called Privacy Statements or Fair Collection notices. See [Example 7](#) for a comprehensive Fair Obtaining Notice.
- 6.5 Ensure that your Protocol establishes which Partner takes the lead in informing individuals (this is usually the Partner who is the first point of contact – this may mean it could be all partners depending on who the service user contacts first). Ensure that the wording to be given to individuals is agreed. It can be presented on a form or in leaflet format. NB: The Data Protection Act does not require us to be so specific and formal when the purpose is transparent. Therefore, each trip to the Doctors does not require the Doctor to show you a form about why s/he needs to take medical details from you. Be pragmatic about this. Any sharing of data between agencies quite often *does* need to be explained.
- 6.6 There are a limited number of situations where you are not required to tell people what you are doing with their personal data, for example where by doing so you could prejudice criminal proceedings or endanger their mental/physical health. Your Standard Lead Officer can advise on this.
- 6.7 Under the DPA, individuals have a right to see personal information held about them. Data Controllers can charge a fee of £10 in most cases, should ensure they can verify the identity of the applicant and must then provide the data subject with a copy of the requested information within 40 days. There are situations when an exemption applies and the personal data can be withheld. Each Partner should have a Data Protection Officer or someone responsible for dealing with these requests. Responsibility for dealing with requests for personal information held as part of the partnership project should be clarified and made explicit in the Protocol.
- 6.8 Each partner should have procedures for dealing with complaints. All Partners should agree to co-operate in order to resolve any complaints relating to the disclosure or the use of personal information that has been supplied or obtained under the Protocol. This responsibility should be included in the Protocol.

Example 7 – Sample Fair Obtaining Notice

WANDS have included the following fair obtaining notice on their registration forms. It clearly meets the criteria of saying who is using the data and for what purpose. It also explains more by saying that sometimes they will ask consent to share and at other times there will be legal reasons for sharing, explained in an accompanying policy:

- *“The information given on this form will be subject to the provisions of the Data Protection Act 1998.*
- *The information you give us on this form will be stored on the WANDS Children’s Centre computer database.*
- *Anonymous data will be used by WANDS and Sure Start for monitoring purposes and in order to improve services.*
- *Information on this Registration Form will only be shared with our partner agencies if you give us your consent by signing the Service Users Consent Form. Other information will be shared in accordance with our Policy for Service Users on Confidentiality and Information Sharing*, which can be found in the WANDS Children’s Centre Reception area.*

If you have any concerns regarding the above procedures, please discuss them with the Programme Manager”.

step

7

Approval, Implementation and Review

- 7.1 The task of writing the protocol must be backed up with a clear plan for approval, implementation and review.
- 7.2 Approval should be straightforward – arrangements for sign-off were agreed in Steps 1 and 2. It should be clear who is responsible for signing up to the protocol from each agency partner. Once the protocol has been signed it can be published – contact your Data Sharing Standard Lead Officer to discuss publishing this on the Partnership website.
- 7.3 A more complex task is making the arrangements for implementation, and particularly, ensuring consistency across partner agencies. If the Protocol is to be a useful process staff members at a variety of levels will need to be briefed and trained within each partner agency. Systems may need to be adapted to reinforce the agreement. You may wish to append an Implementation Plan to your Protocol.
- 7.4 Staff members will need to understand the legal basis for sharing information, arrangements for consent, practical procedures for what can be shared with whom, and arrangements for communicating with the individuals whose information is collected. Information materials for staff may be best developed over a period of time. A short pilot period of 3 months could be used to introduce operational staff to the protocol arrangements and to work with them to develop practical materials to reinforce its use.
- 7.5 The Protocol should contain a regular review period, usually annually, but may be shorter/longer depending on the nature of the project. (If a pilot is used, the first review should occur at the end of the pilot period). Where possible, the original Protocol Working Group should perform the review. In the absence of the Group, the relevant Data Sharing Standard Lead Officers should prompt the review.
- 7.6 The review should consider whether the Protocol has worked in practice; whether all the Partners met their agreed responsibilities; and whether problems have occurred and how they might they be rectified. The key purpose of the review is to strengthen the arrangements for sharing personal information. The review may also be an appropriate time to check accuracy of personal data held, and refresh consent where necessary (if consent has been obtained). Where any changes are made to the Protocol the signatures of all the protocol partners should be gained again.
- 7.7 If during Review it is clear that the need for information sharing has ended, the Protocol should be terminated, the register amended and all Partners informed.
- 7.8 If at any time a Partner identifies a breach of a Protocol, this should be discussed and steps taken to rectify the problem. For any problems encountered whilst developing an Information Sharing Protocol, please contact your Data Sharing Standard Lead Officer or Data Protection Officer (if the two are different).

What did the pilot projects suggest to help implementation and review?

The Pilot protocol leads suggested various ways of implementing Protocols once they have been developed:

- *‘Once signatures are gained, tell everyone involved that the Protocol exists!’*
- *‘Hold a workshop to launch the Protocol and explain its practical use – this needs to be mandatory for all staff involved – and needs to be available for new staff. The workshop should be practical and include scenarios where the Protocol would kick in. Make it fun – use quizzes’*
- *‘Senior managers need to be seen to own this’*
- *‘An implementation plan is required, making clear who owns it and what happens at each stage’*
- *‘You could create a mini training pack’*
- *‘Always build in a review date and involve the right people’*
- *‘Learn from other implementations that haven’t worked and do not make the same mistakes!’*

checklist

Once you've completed this Toolkit, the following will act as a checklist

- **Have you got all the Partners together?**
- **Have you registered your work with your Data Sharing Standard Lead Officer?**
- **Do you need to develop a business case to gain approval and decide who will sign the Protocol in each agency?**
- **Have you specified your purpose?**
- **Is someone leading the development of the Protocol?**
- **Have you planned who needs to share what with whom?**
- **Have you a Data Protection condition for this?**
- **Have you a legal power to rely on?**
- **Have you checked you are not breaking any laws?**
- **Have you complied with the Human Rights Act?**
- **Have you followed the consent guidance, if you are using consent?**
- **Are you clear about how records will be managed and kept secure?**
- **Have you communicated your sharing to the users of your services?**
- **Have you had the protocol signed off?**
- **Have you created an implementation plan for the protocol which involves training all staff (and new staff) who need to know?**
- **Have you scheduled a review date?**

Appendix A

Explanation of Terms

This guidance uses terminology from the Data Protection Act 1998 with which you may not be familiar. The list below aims to explain these terms.

Caldicott Guardian

A senior health or social care employee who has a strategic role for the management of patient/client information, including agreeing and reviewing protocols governing the protection, use and disclosure of patient information.

Data Controller

The person (usually a Body) who determines the purposes for and the manner in which personal data are processed. Data Controllers must comply with the Data Protection Act. In a partnership, it may be that all partner bodies are Data Controllers.

Data Processor

Any person (individual or body, other than an employee of the Data Controller) who processes data on behalf of the Data Controller. For example, if a Partner out-sources a function, such as debt collection, to an outside agency, then that agency is a Data Processor, working on the Data Controller's behalf.

Data Subject

An individual who is the subject of personal data. This could be a member of the public or an employee of the Partner's organisation.

Fair Obtaining Notice

Unless an exemption applies, the data subjects must be given certain information about the processing of their personal data, at the point of collection. The key elements of this are the identity of the data controller, the purposes of the processing and anything else necessary to guarantee fairness (this may include disclosures, how long their data will be retained)

Personal Data

Data relating to an individual who can be identified from those data, or from those data together with any other information in the possession of (or likely to come into the possession of) the Data Controller. Therefore, for example, if we can put a payroll number and a name together, we have personal data.

Processing

Obtaining, recording, holding, organising, adapting, retrieving, consulting, disclosing, aligning, blocking, erasing or destroying the data. Processing effectively means doing anything with data.

Sensitive Personal Data

The DPA defines *sensitive personal data* as personal data consisting of information as to

- the racial/ethnic origin of the data subject
- his/her political opinions
- his/her religious or similar beliefs
- his/her membership of a trade union
- his/her physical or mental health or condition
- his/her sexual life

- the commission or alleged commission by him/her of an offence and any related proceedings

All personal data should be treated with care.

Subject Access Requests

Data Subjects have a right to ask to see and have copies of information held about themselves. To exercise this right, the Data Subject can make a Subject Access Request. Contact Partner Data Protection Officers for information on dealing with these requests.

Third Parties

In relation to personal data, third party means any person other than the Data Subject, the Data Controller (including employees), or any Data Processors (including employees)

The Data Protection Principles

There are 8 Data Protection Principles. These form the backbone of the Act and are referenced throughout this guidance. In summary, the Principles are as follows:

1. Personal data must be processed fairly and lawfully and that processing must satisfy at least one of the conditions in Schedule 2 of the Act. If sensitive data is being processed, then at least one condition in Schedule 3 must also be satisfied.
2. Personal data shall be obtained for only one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes
3. Personal data shall be adequate, relevant and not excessive for the purposes
4. Personal data shall be accurate and, where appropriate, kept up to date
5. Personal data shall not be held for any longer than is necessary
6. Personal data shall be processed in accordance with the rights of the data subject
7. Appropriate technical and organisational measures shall be taken to protect personal data
8. Personal data shall not be transferred outside the European Economic Area unless adequate protection is provided

For further explanation of the Principles, please contact Partner Data Protection Officers

Appendix B: Templates for Tier 2 and Tier 3 Protocols.

Template for Tier 2 ‘general’ information sharing protocols.

Information Sharing Protocol to provide the framework for detailed information sharing agreements concerning *[enter broad community here]*

1. Contents

-
-
-
-

2. Partner agencies covered by this protocol

Agency (Division / section / team)	Protocol Lead person (Name & job title)	Protocol signatory (Name & job title)

3. Relationship of this Protocol to other Protocols:

This Protocol sits at Tier two in a framework for Worcestershire. Its relationship to other protocols can be seen in the table below:

Tier One	Worcestershire Standard for Sharing Personal Data
Tier Two	<i>[Enter title of this Protocol]</i>
Tier Three	<i>[Enter details of any Tier 3 Protocols that are being planned]</i>

4. Agreed approach to information sharing in the xxxxxxxxxx community

Any Tier Three Information Sharing Protocol created as a sub-set to this Protocol will adhere to the following criteria:

Principles, ethics and professional practice	<ul style="list-style-type: none"> • • • •
Agreed Terminology	<ul style="list-style-type: none"> • • • •
Defining local variations	<ul style="list-style-type: none"> • • • •

4.What is the legal basis for this sharing?(this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

Acts	Further details

All information shared for the purpose of this protocol should be accurate, current and should not be shared indefinitely. The quantity and coverage of data shared should be directly related to the purpose of sharing, and not excessive.

5.Processes for informing individuals about use of their data (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

6.Processes for dealing with Subject Access Requests and Complaints (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

7.Processes for informing and guiding staff about the arrangements (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

8. Additional requirements, including security (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

9. Templates (insert any templates, such as for consent, as appendices) (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

10. Implementation Plan (create and insert a local implementation plan as an appendix) (this is sometimes appropriate at Tier 2, or sometimes at Tier 3)

11. Processes for informing and guiding staff about the arrangements

12. Partner sign off

This Protocol applies from..... *[enter date]* 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:

Agency	Name and job title	Signature

Template for Tier 3 ‘practical’ information sharing protocols.

Information Sharing Protocol to *[enter broad purpose here]*

1.Contents

-
-
-
-

2.Partner agencies covered by this protocol

Agency (Division / section / team)	Protocol Lead person (Name & job title)	Protocol signatory (Name & job title)

3.Purposes of sharing information covered by this protocol

-
-
-

The information covered by this protocol can only be used for the purpose for which it was collected. If any of the Partners to the protocol want to change the purpose, all Partners need to agree to the change. If a Partner to the protocol wants any of the data for further statistical purposes, personal information should be anonymised.

This protocol has been developed bearing in mind the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000.

4. Relationship of this Protocol to other Protocols:

This Protocol sits at Tier three in a framework for Worcestershire. Its relationship to other protocols can be seen in the table below:

Tier One	Worcestershire Standard for Sharing Personal Data
Tier Two	<i>[Enter any 2nd tier protocol that exists]</i>
Tier Three	<i>[Enter name of this Protocol]</i>

5. Specific information which will be shared

[Help](#)

Data Categories	May include....

6. What is the legal basis for this sharing?

[Help](#)

Acts	Further details

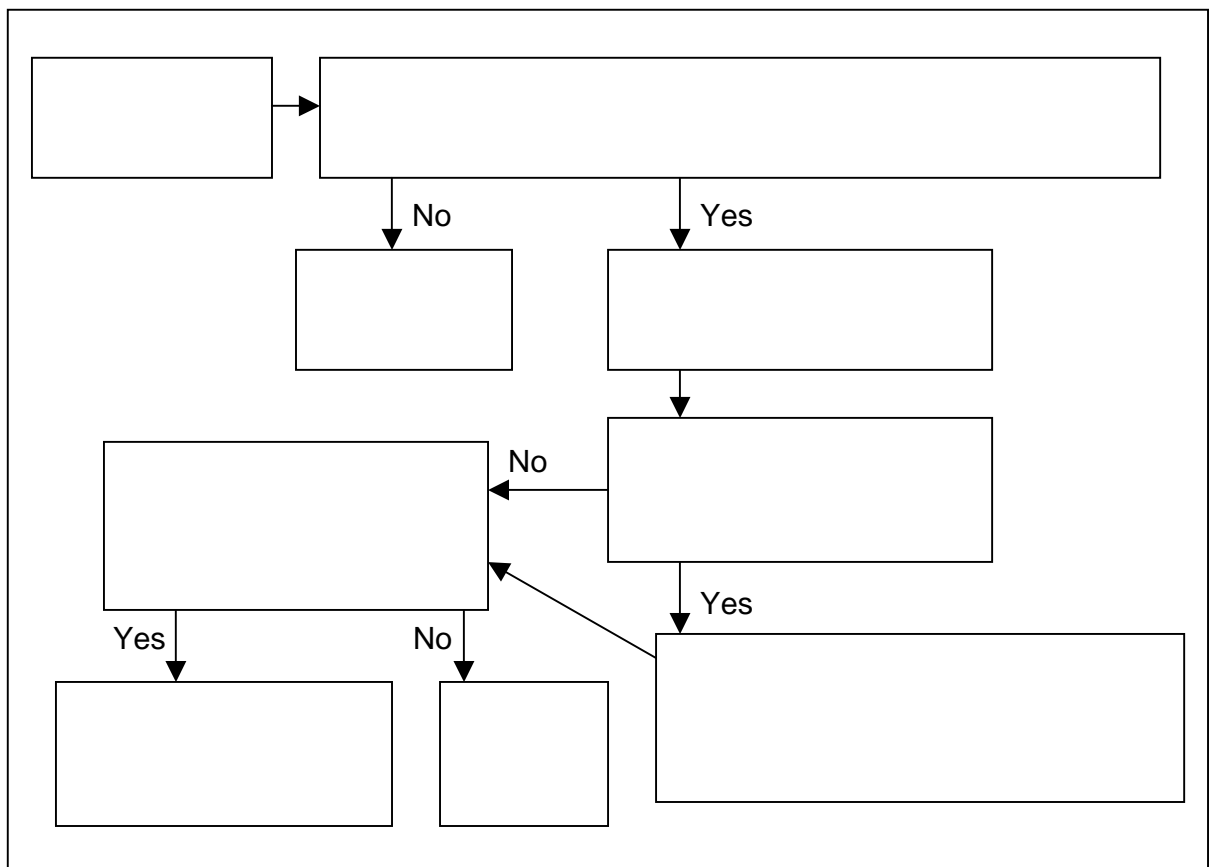
All information shared for the purpose of this protocol should be accurate, current and should not be shared indefinitely. The quantity and coverage of data shared should be directly related to the purpose of sharing, and not excessive.

7. Processes for sharing the information

[Help](#)

Data Category	Partner collecting this information	Partner receiving the information	DP Condition for sharing	Caveats on the sharing	Retention periods

Or



8. Processes for informing individuals about use of their data (this may have been covered at Tier 2 – if a Tier 2 Protocol exists)

9. Processes for dealing with Subject Access Requests and Complaints (this may have been covered at Tier 2 – if a Tier 2 Protocol exists)

10. Processes for informing and guiding staff about the arrangements (this may have been covered at Tier 2 – if a Tier 2 Protocol exists)

11. Additional requirements, including security (this may have been covered at Tier 2 – if a Tier 2 Protocol exists) [Help](#)

12. Templates (insert any templates, such as for consent, as appendices)

13. Implementation Plan (create and insert a local implementation plan as an appendix)

14. Partner sign off

This Protocol applies from..... *[enter date]* 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:

Agency	Name and job title	Signature

Help: Example of specific information that will be shared [Back to Section 5](#)

Example Data Categories	May include....
Financial details	Bank account details
Crime details	Allegation made, name of alleged victim, name of offender
Personal details about parent / carer.	Name, address, telephone number, Employment status.
Sensitive personal details about child / children (as defined by Data Protection Act 1998)	Health details (GP practice, health visitor, midwife, mental / physical health), ethnicity. plus whether has a disability or special need. Back to Section 5

Help: Examples of Legal bases for sharing this information [Back to Section 6](#)

Acts	Further details
Children Act 1989	“All agencies must consider whether they need to consult with or refer to Social Services, a child who is in need (S17) or a child who is / may be suffering significant harm (S47). They must also consider whether information coming to their attention about children resident in Worcestershire indicates the need for an enquiry to the Child Protection Register” (Worcestershire ACPC Inter-Agency Guidance).
Children Act 2004	Section 10: “Each Children’s Services Authority in England must make arrangements to promote co-operation ... with a view to improving the well-being of children.
Local Government Act 2000	Section 2: “ Every local authority are to have the power to do anything which they consider is likely to achieve any one or more of the following objects:- (a) the promotion or improvement of the economic well-being of their area. (b) the promotion or improvement of the social well-being of their area, and (c) the promotion or improvement of the environment well-being of their area.” Back to Section 6

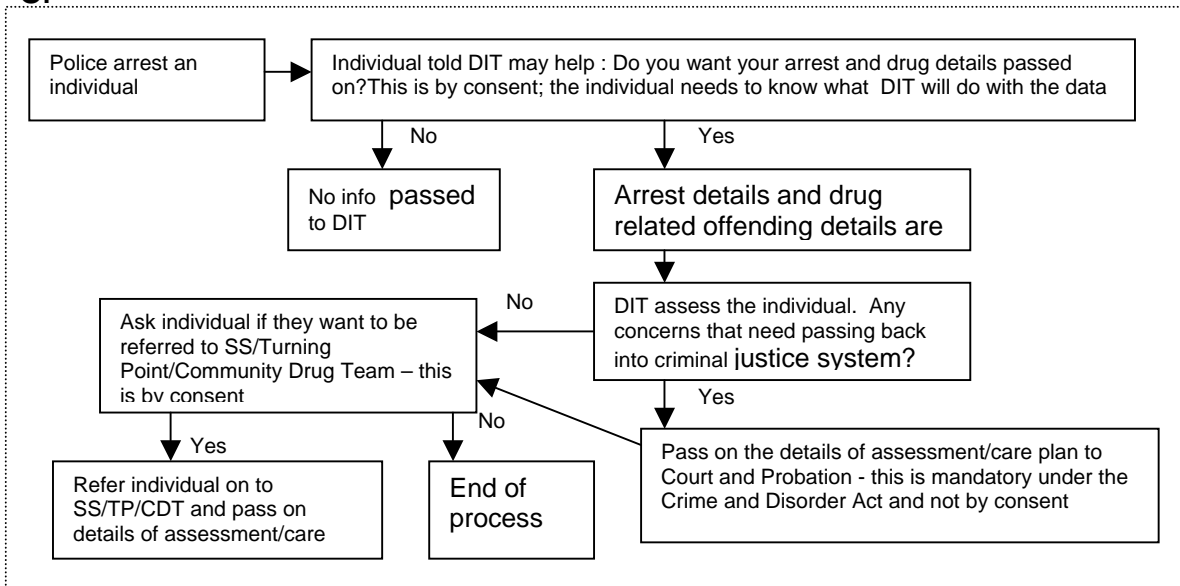
Help: Examples of Processes for sharing the information

[Back to Section 7](#)

This table is an example only – you may wish to create a different table, or perhaps a flowchart to show how the information is passed from one Partner to another. The important thing to remember is that you know whether it is by consent or under a legal obligation. or another condition.

Data Categories	Data held by	Data shared with	DP Condition
Details of arrest / Drug related offending	Police	DIP Team	Consent
Details of Assessment and Care plan	DIP Team	Probation service Court service Social Services Turning Point CDT	Legal* Legal* Consent Consent Consent
Details of Sentence	Court Service	Probation service Prison service DIP Team	Legal* Legal* Legal*
Details of release from prison inc early release	Prison service	DIP Team Probation	Legal* Legal*
Details of Completion of Community sentence	Probation service	DIP Team CDT Turning Point	Legal* Consent Consent
Details of leaving Treatment planned/ unplanned	CDT Turning Point	DIP Team	Consent

Or



[Back to Section 7](#)

Help: Additional requirements

[Back to Section 11](#)

This section can be used to describe any specific security requirements, not identified in the overarching protocols and only relevant to this protocol, or additional arrangements for notification of the Information Commissioner (ie: if the activity is not covered by their organisation’s existing notification).