



Information-Sharing Code of Practice August 2017

1 Introduction

Information sharing is a vital part of ensuring that professionals can effectively assess the needs of a child or the risks to a child. Often it is only when information from a number of sources has been shared that it becomes clear that a child has suffered, or is likely to suffer, significant harm. Early sharing of information is also the key to providing effective Early Help where there are emerging problems. Serious Case Reviews (SCRs) have shown how poor information sharing has contributed to the deaths or serious injuries of children, and Working Together 2018 is absolutely clear that *“Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe.”*

The purpose of this Code of Practice is to outline the principles and practice which govern the sharing of information between agencies, for the purposes of safeguarding and promoting the welfare and protection of children and young people. The appendices provide some additional guidance to assist professionals with decision making around information sharing.

It is expected that agencies and professionals working with children and families in Buckinghamshire adhere to this Code of Practice and supply information within the bounds of this Code. This will help ensure the right help and support can be provided at the right time, and that the best outcomes are achieved for children and families. BSCB partner agencies will be asked to re-affirm their commitment to this code through signing the [BSCB Member Compact](#) on an annual basis.

There has been an update following the introduction of General Data Protection Regulations (GDPR).

The Board has considered what changes are required to the Procedures to ensure compliance with the General Data Protection Regulations (GDPR) - implemented through the Data Protection Act 2018. We have taken into consideration guidance from the Information Commissioner’s Office [ICO] which says: ‘The biggest change is for public authorities, who now need to consider the new ‘public task’ basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests’. As a result, the Board recommends that ‘legal obligation’ and ‘public task’ (as defined in the GDPR) are relied on as the primary basis for processing information to establish whether or not there is a need to safeguard the welfare of a child. This means that, whilst families will be informed when personal data is being shared or processed, their consent is not required.

The significance of this change is that it is no longer necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child (i.e. removing the distinction between information sharing for the purposes of assessing need or child protection). It does, of course, continue to be good practice to inform parents / carers that you are sharing information for these purposes and to seek to work cooperatively with them. Agencies should also ensure that parents / carers are aware that information is shared, processed and stored for these purposes.

The Working Together Guidance published in July 2018 by the Department for Education, continues to emphasise the use of consent. The BSCB is working to ensure that the approach

taken in these Procedures is consistent with the Data Protection Act 2018, the guidance published by the ICO and the statutory guidance published by the Department for Education. In the meantime, references to consent and information sharing in the Procedures will be highlighted with a link to the advice above. In addition, the information sharing protocol has been withdrawn pending a full revision in line with the new legislation.

This Code of Practice should be read in conjunction with:

- [The Information Commissioner's Office Data Sharing Code of Practice](#): This is a statutory code which explains how the Data Protection Act applies to the sharing of personal data. It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one off requests to share personal data.
- [The Government's Information Sharing Advice for safeguarding practitioners](#): This advice is for front-line practitioners and senior managers. It helps them decide when and how to share personal information legally and professionally.

Alongside this Code of Practice, individual agencies should also refer to their own Information Governance Policy and any other organisational or sector specific guidance.

Whilst this Code of Practice provides a framework and set of principles for sharing information to safeguard and promote the welfare of children and young people, more detailed information sharing agreements may need to be drawn up between individual agencies or groups of agencies for specific purposes. An example information sharing agreement is provided at Appendix 3 and can be used and adapted by agencies operating in Buckinghamshire. This should always be done with support from relevant organisational information sharing leads.

2 The Legal Framework

In addition to the statutory guidance following from the [Children Act 2004](#), the key legal concepts, legislation and terminology relevant to information sharing are contained in:

- [The Data Protection Act 1998](#) (and from 25th May 2018, the General European Data Protection Regulations. This Code will be reviewed in January 2018 in anticipation of these new regulations.)
- [The Human Rights Act 1998](#)
- [The common law duty of confidentiality](#)

3 Information Sharing Responsibilities

Responsibilities of the Buckinghamshire Safeguarding Children Board (BSCB)

The BSCB is responsible for:

- Ensuring this Code is regularly reviewed and kept up to date
- Disseminating relevant learning in relation to sharing and storing information, for example learning that arises from the resolution of concerns, from Serious Case Reviews, auditing or other quality assurance activity
- Ensuring that BSCB multi-agency training supports the effective implementation of this Code. This includes ensuring that the key principles of this code are embedded across BSCB training courses and considering the provision of specific information sharing learning / training
- Ensuring that relevant concerns, risks or areas of good practice in relation to sharing or storing information are discussed through the BSCB and its Sub Groups and that any appropriate action is agreed and taken.
- Using the BSCB quality assurance framework to review whether agencies are effectively sharing and storing information. This includes using the Section 11 auditing framework to assess whether partners have effective mechanisms in place to ensure information is shared and stored in line with this Code
- Where necessary, seeking additional legal or specialist advice and guidance to support multi-agency discussion around effective information-sharing.

Responsibilities of agencies

All agencies (statutory and non-statutory) working with and / or providing services for children and young people in Buckinghamshire are responsible for:

- Contributing to the development of trust and confidence between agencies by working within the framework of this Code

- Having effective mechanisms in place to ensure this Code is fully implemented, and that staff and volunteers know of its existence
- Ensuring that all staff and volunteers who are in contact with children understand what to do and the most effective ways of sharing information if they believe that a child and family may require a particular service in order to achieve positive outcomes. This includes being able to understand and apply good practice in sharing information at an early stage as part of early help or preventative work
- Ensuring that all staff and volunteers who are in contact with children understand what to do and when to share information if they believe that a child may be a child in need or a child who has suffered / is likely to suffer significant harm
- Ensuring appropriate agency or sector specific guidance is available to complement this Code and the government guidance
- Ensuring that an appropriate level of training on information sharing is made available to staff as part of their induction and ongoing training
- Ensuring that any problems encountered by staff in relation to the sharing or storing of information are recorded, and that this is reviewed on a regular basis to identify any concerns
- Ensuring that requirements in relation to information sharing are embedded into commissioning processes and effective monitoring of service level agreements
- Analysing any complaints relating to information sharing in order to improve practice, and where relevant sharing learning with the BSCB for wider dissemination
- Ensuring that any reported breaches of the code are followed up in accordance with this Code and internal procedures
- Sharing improvements that have been made in relation to information sharing with the BSCB so that relevant learning can be shared across the partnership
- Supporting common systems and joint approaches that will promote effective information sharing between agencies
- Being transparent around information sharing and encouraging children and their parents to see information sharing in a positive light, as something which makes it easier for them to receive the services they need
- Ensuring that the organisation is properly registered with the Information Commissioner
- Ensuring that requests and responses to requests are sent by a secure method agreed between the services
- Ensuring that information is not kept for longer than is necessary and that there is adherence to agency or sector specific retention schedules.

Each agency should have in place a lead information officer who is responsible for decisions relating to information sharing within the agency, or between the agency and a third party and who can assist in the resolution of challenges as well as providing advice and guidance.

Responsibilities of professionals

All professionals (including volunteers) working with children and young people in Buckinghamshire are responsible for:

- Adhering to this Code and sharing information in line with this Code. This includes clearly recording decisions about whether or not to share information.
- Raising with their line manager / safeguarding lead any training or learning requirements in relation to information sharing
- Recording and raising with their line manager / safeguarding lead any breaches of this Code or any concerns about the way information is being shared and stored either within their own agency or in other agencies.
- Ensuring that anyone who provides personal information is given details of how that information may be used, made aware of their rights in relation to information disclosure and their right of access to information they have provided, and given details of how to make a complaint.

No professional should assume that someone else will pass on information which they think may be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to suffer harm, they should make a referral to Children's Social Care in line with BSCB procedures.

Responsibilities of Agents and Sub-contractors

Each agency shall ensure that its commissioning arrangements comply with this Code. Commissioning and contract monitoring processes should allow commissioners to have assurance that services are being delivered in line with this Code.

Commissioned services and professionals working within commissioned services have the same responsibilities as those of agencies and professionals set out above.

4 Disagreement around Information Sharing

Where there is disagreement between professionals or agencies about the way information is being shared or in relation to a decision not to share information, the BSCB Escalation and Conflict Resolution Procedure should be followed.

5 Complaints and Breaches

Breaches reported by a member of the public will usually present as a complaint. Every organisation should have their own complaints procedure, which should be adhered to should a member of the public report an incident.

Each organisation should have an information governance policy which should be compliant with current legislation including the Data Protection Act and (from 25th May 2018) the GDPR. Any inadvertent disclosure of information by an employee must be investigated in line with internal procedures.

Further information on [how to manage a data protection breach](#), including how to report a breach is available from the Information Commissioner's Office.

In order to be able to monitor adherence to the Code, as effectively as possible and to consider remedial action where appropriate, it is important that information on all breaches is collated. Procedures should therefore be put in place within each organisation to ensure that details of complaints relating to the inappropriate disclosure of information (and the outcomes) are collated and reviewed on a regular basis.

Each agency will be held responsible for any misuse of the information supplied to it and the consequences of such misuse by its employees or agents.

Appendix 1: Guidance to assist with decision making in relation to sharing information

Effective interagency working is dependent upon appropriate and timely information sharing whether a child or young person just needs some additional support (Early Help) or whether there are concerns that they are at risk of significant harm (safeguarding).

The Information Commissioner's Office has produced some [case studies](#) that present a number of different scenarios relating to information sharing. These practical examples may be helpful for individual professionals when making decisions around information sharing, or could be used as a resource for training or group discussion.

Early Help

In Buckinghamshire, Early Help includes any help or support that is provided to a child or family across levels 1-3 of our [Thresholds document](#). At this level, a child or family may have complex and /or multiple needs but the threshold for statutory intervention led by Children's Social Care has not been met. This means the child is not assessed to be at risk of significant harm.

At this level of need freely given, informed explicit consent is needed. Where a professional believes they need to share information to help them understand the needs of a child / family, or to enable the child / family to receive a service from another agency, they should seek consent from all the relevant individuals before information is shared or requested. This will ensure that the child / family understand the issues and it will support good engagement by the child / family with services.

Safeguarding

If a professional has a safeguarding concern about a child, they should discuss with their line manager or designated safeguarding lead without delay to agree the most appropriate course of action.

If there is reasonable cause to believe that the child has suffered, or is likely to suffer significant harm, then consent is not required in order to make a referral to Children's Social Care. However, in most cases it remains good practice to obtain consent (which should be freely given, informed and explicit), and professionals should still seek to discuss their concerns with the family and seek their agreement to making a referral to Children's Social Care. This will help the family to understand the concerns and why they will be contacted by Children's Social Care.

In some situations it may be unclear whether or not the threshold for referral to Children's Social Care has been met. In these situations, the concern must not be ignored. Professionals should talk to their agency's designated safeguarding lead and, if necessary their lead officer for information sharing to assist with decision making. The safety and wellbeing of the child must be the overriding consideration in making any decisions whether or not to seek consent.

When not to seek consent

There are a limited number of circumstances where professional **should not** seek consent e.g. where to do so would:

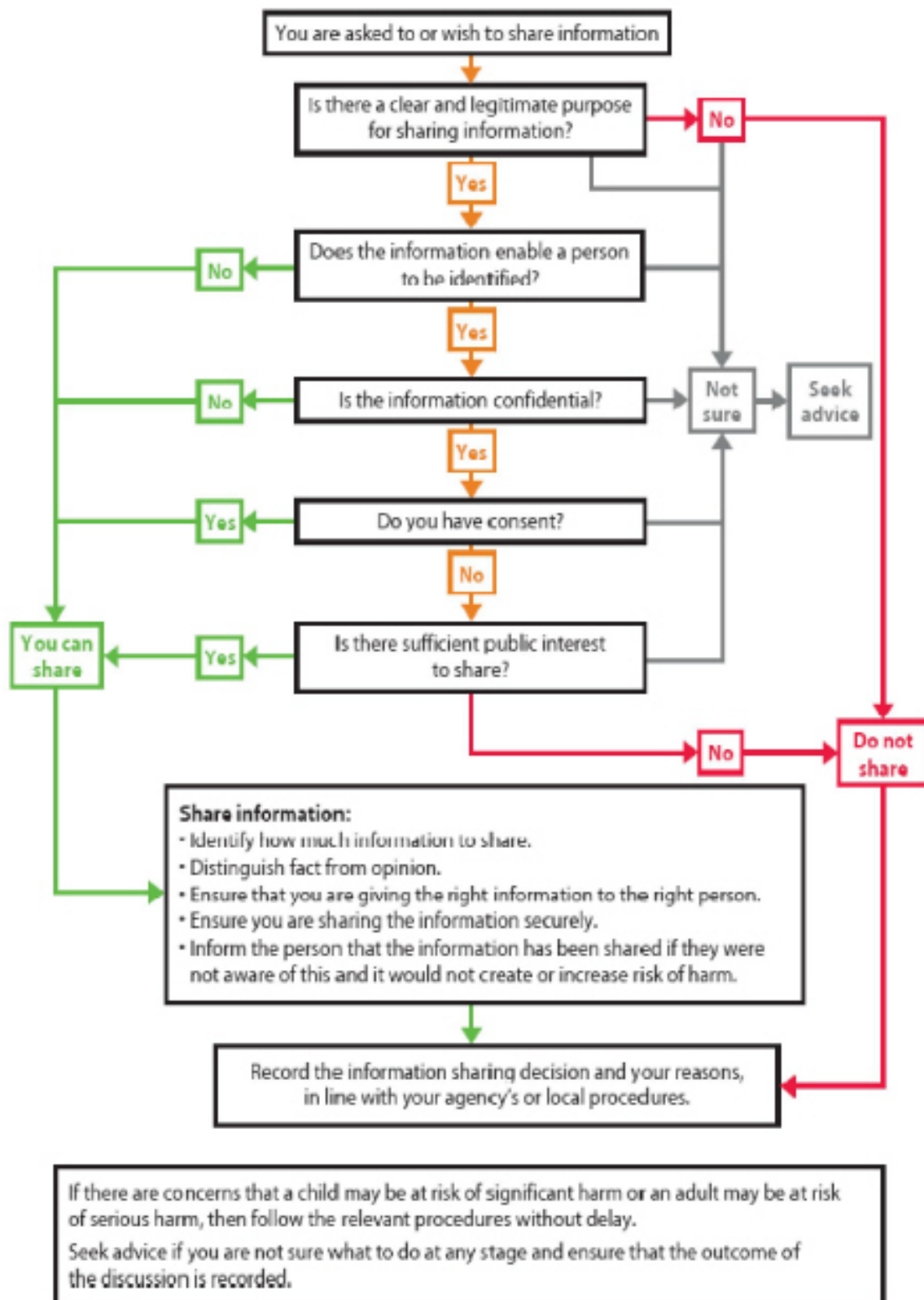
- Place a child at increased risk of significant harm
- Place an adult at risk of serious harm
- Prejudice the prevention or detection of a serious crime
- Lead to unjustified delay in making enquiries about allegations of significant harm.

If a professional shares information without seeking consent, this should be clearly recorded, including the reasons for not seeking consent. Recording should set out the legal basis under which information is being shared.

It is important that all professionals who have contact with children and families are able to have conversations about consent. Not gaining consent where it is needed can cause delay in children and families accessing services that will help meet their needs.

Decision Making

In deciding whether or not to share information it may be helpful for professionals to refer to the following decision making flow chart. A more detailed explanation of the questions and the terms used within them is set out after the flow chart.



1. Is there a clear and legitimate purpose to share the information?

The following questions can be helpful in establishing whether there is a clear and legitimate purpose for sharing information.

- Is there a legal basis or statutory duty for sharing the information? (e.g. s47 of the [Children Act 1989](#) or a court has made an order for certain information or files to be brought before the court)
- Is the request proportionate to the purpose for which disclosure is sought?
- Why is the information being shared or requested?
- Can either party, requesting or sharing the information, show a sufficient 'need to know'?
- Was the information obtained under a specific statutory power or duty which limits what can be done with it and who the information can be shared with?
- Will the request involve secondary disclosure? (Disclosure by the person to whom data has been disclosed to another agency or person e.g. if a GP provides data to a school and the school passes it to Children's Social Care)
- Is there another way to achieve the objective with less impact on confidentiality? (e.g. would anonymous data suffice?)

2. Does the information enable a person to be identified?

In most cases where information is shared at an operational level it will be about a named child. It may also identify others, such as a parent, carer or other family members.

However, there will be other scenarios where anonymised information will be sufficient. For example anonymised data may suffice for the purpose of data analysis or report writing. The Buckinghamshire Safeguarding Children Board maintains a multi-agency dataset, which helps the Board to have assurance around safeguarding practice and the outcomes achieved for children across the partnership. This includes a range of anonymised and aggregated data from across partners, as data which personally identifies the individuals involved is not necessary to undertake the required analysis.

If the information is anonymised, it can lawfully be shared as long as the purpose is legitimate. If the information allows a child and others to be identified, it is subject to data protection law and professionals must follow this Code of Practice and where appropriate take legal advice in deciding whether or not to share the information.

3. Is the information confidential?

Confidential information is information of some sensitivity, which is not already lawfully in the public domain or readily available from another public source, and which has been shared in a

relationship where the person giving the information understood that it would not be shared with others.

There is a common law duty of confidentiality when dealing with sensitive personal data. A breach of confidence will not occur if there is a recorded legitimate purpose to share, or if there is evidenced that freely given, explicit informed consent has been obtained.

4. If the information is confidential, has consent to share been obtained?

Consent must be freely given, informed and explicit. This means that the person giving consent needs to understand why information needs to be shared, who will see their information, the purpose for which it will be used and the implications of sharing that information.

The ICO provides further guidance on [what is meant by 'consent'](#).

Professionals need to consider whose consent should be sought. Where there is a duty of confidence, it is owed to a person who has provided the information on the understanding it is to be kept confidential and, in the case of medical or other records, the person to whom the information relates.

The law does not set out a specific age at which children should be asked for consent. 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 to sharing.

In most cases, where a child cannot consent, or where a professional judges that they are not competent to consent, a person with parental responsibility should be asked to consent on behalf of the child. However, the capacity of the parent to consent also needs to be taken into consideration.

In relation to both children and adults with parental responsibility, professionals should refer to the [Mental Capacity Act 2005](#) and their own agency or sector specific guidance in determining capacity to consent. If there is any doubt, or in case where there is conflict between the wishes of the parent and the child or two adults with parental responsibility, then professionals should seek guidance from their safeguarding lead.

When a professional seeks consent for information to be shared, the following information should be provided as a minimum:

- What information has been or will be collected
- The purposes for which it will be used
- Who the information might be shared with
- The purposes for which the agencies that receive the information might use it (including detection of crime).

The need to renew consent should be reviewed and professionals should be aware that individuals have the right to withdraw consent after they have given it.

All sharing of sensitive information, even where there is consent, should be recorded including the legal basis for sharing information and the decision making process for deciding that information should be shared.

5. If consent has been refused, or there are good reasons not to seek consent to share confidential information, is there a sufficient public interest to share information?

Even where sharing of confidential information is not authorised, professionals may lawfully share it if this can be justified in the public interest. A public interest can arise in a range of circumstances e.g. to protect children or other people from harm, to promote the welfare of children or to prevent crime and disorder. In making a decision about whether there is sufficient public interest to share information, professionals 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 a reasonable judgement.

Where there is a clear risk of significant harm to a child, or serious harm to adults, the public interest test will almost certainly be satisfied. There will be other cases where professionals will be justified in sharing some confidential information in order to make decisions on sharing further information or taking action - the information shared in such circumstances should be proportionate.

Circumstances in which sharing confidential information without consent will normally be justified in the public interest are:

- When there is evidence that the child has suffered, or is likely to suffer, significant harm
- Where there is reasonable cause to believe that a child has suffered, or is likely to suffer, significant harm
- To prevent significant harm arising to children or serious harm to adults, including through the prevention, detection and prosecution of serious crime (serious crime means any crime which causes or is likely to cause significant harm to a child or serious harm to an adult).

In deciding whether the public interest justifies disclosing confidential information without consent, professionals should be able to seek advice from a line manager or designated safeguarding lead.

If professionals decide to share confidential information without consent, this should be explained to the child or their parent, unless to do so would put the child at risk of harm.

Professionals must record the context in which the information was shared, the legal basis for sharing information the perceived level of risk of harm at the time, the data requested, the data shared and with whom. Agencies may have a standard form for this or ensure that there is a signed and dated entry in the case notes.

6. If the decision is to share, is the right information being shared in the right way?

If the decision is to share, professionals should share information in a proper way. This means:

- Share the information which is necessary for the purpose for which it is being shared
- Share the information with the person or people who need to know
- Check that the information is accurate and up-to-date
- Share it in a secure way
- Establish with the recipient whether they intend to pass it on to other people
- Ensure they understand the limits of any consent which has been given
- Inform the person to whom the information relates, and, if different, any other person who provided the information, if professionals have not already and it is safe to do so.

7. Have the decision and the reasons for it, been recorded?

Professionals should record all decisions whether or not to share information and why. If the decision is to share, the record should include what information was shared and with whom, and who gave consent (dated and timed)

Appendix 2: Seven Golden Rules for Information Sharing (Taken from HM Government Statutory Guidance on Information Sharing)

Seven Golden Rules for Information Sharing

1. Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix 3: Template Information Sharing Protocol

This template can be used by agencies which need to put in place a specific information sharing protocol to govern the way information is shared for a specific purpose. The template **MUST** be completed and agreed in consultation with your agency's lead officer for information sharing.

Description of data flow:	
Date:	
Version:	
Information Asset Owner sharing data:	
Information Asset Owner receiving data:	
Purpose for sharing:	
Type of information:	
Legal basis for sharing	

Data sets: (details may be supplied on a separate sheet if necessary)	
How will the data be transferred? (details may be supplied on a separate sheet if necessary)	

How and where will the data be stored?	
Limitations to use:	
Duration of this DSP:	
How will the data be	

disposed of or destroyed on completion of this term?	
--	--

Privacy Impact Assessment (PIA): (attach PIA or give details)	
---	--

Contact details for persons who can be contacted regarding this protocol	Organisation	Contact

For data sharer(s)	Date
Name:	
Position: (Usually SIRO)	
Signature:	

For data receiver(s)	Date
Name:	
Position : (Usually SIRO)	
Signature:	

Any Supporting documents	
--------------------------	--