HUMBERSIDE POLICE

INFORMATION SHARING POLICY

November 2007

Humberside Police Information Sharing Policy

Contents

Humberside Police Information Sharing Policy

1. Policy Scope

1.1 This policy applies to all Humberside Police staff, whether working on Humberside Police premises or remotely. It also applies to members of other organisations who are authorised to process Humberside Police information, including members of partner organisations.

1.2 The policy covers the sharing of personal data, as defined in the Data Protection Act 1998 (DPA). This Act is intended to protect the rights of individuals when their information is processed. Personal data held by Humberside Police must be processed within the terms of the DPA. Non-personal information is not subject to the same tests or considerations and is routinely shared, e.g. crime rates and performance data.

1.3 Even where legislation is present and indicates that there is a power to share information, it may not give authority to disclose information under all circumstances. Information sharing should not be undertaken as a matter of routine; rather each case must be assessed individually with informed decisions being made about whether or not to share.

1.4 This policy only applies to information processed by Humberside Police for a policing purpose. as defined by the Management of Police Information (MoPI) Code of Practice, i.e.:

- protecting life and property
- preserving order
- preventing the commission of offences;
- bringing offenders to justice
- any duty or responsibility arising from common or statute law.

It refers to any verbal, written, electronic, digital, magnetic or paper based information, including photographic and other optical media. For the purpose of this document, the term ‘information sharing’ can include ‘dissemination’ and ‘disclosure’.

1.5 This policy does not however, cover the Criminal Records Bureau’s Quality Assurance Framework or the sharing of material in connection with criminal proceedings as defined in the Criminal Procedure and Investigations Act 1996, nor does it conflict with any existing arrangements to protect sensitive information.

1.6 This policy does not preclude the sharing of information between police forces for a policing purpose (see paragraph 1.4 above).

1.7 This policy does not preclude the capability for urgent sharing of information to safeguard children and vulnerable adults (see paragraph 3.8).

1.8 Whilst information shared under the terms of this policy will be for a specific purpose, it should be recognised that it may be a valuable source of intelligence for the force and as such should, where appropriate, be managed in accordance with force procedures concerning the recording of intelligence.

2. Policy Aims and Objectives

Aims:

2.1 Effective policing relies on the force communicating and sharing information with a wide range of partners. The purpose of this document is to ensure that the sharing of police information with partners is carried out in an accurate, adequate, timely and lawful manner by Humberside Police.

2.2 There are significant benefits which accrue from sharing information between partners to achieve a common purpose. These include:

- improving public services through an increased capability of all stakeholders to make informed decisions about how best to protect the public
- assisting operational policing by creating a two-way process that enables links to be made between people, objects, locations and events
- increasing expertise, professionalism and understanding of the process of sharing information
- increasing openness and transparency amongst partners which in turn, builds confidence and trust in the police service.

2.3 This is the overarching policy outlining the management of Information Sharing Agreements (ISAs) between Humberside Police and its partners.

2.4 The contents of this policy and its associated procedural instructions are intended to protect Humberside Police by minimising the risks posed by entering into informal and unregulated ISAs.

2.5 This policy aims to preserve:

- the confidentiality of information by ensuring it is only accessible by those who have been authorised to have such access, and by ensuring

- the integrity of the information by safeguarding the accuracy and completeness of both the information and the processing methods utilised
- the availability of the information by ensuring that authorised users have access to information and other assets when required
- the continued management of information shared using the Management of Police Information (MoPI) Code of Practice and Guidance.

Objectives:

2.6 In order that the above aims are met, the force will:

- ensure that all the information is processed with due regard to the rights of the individual, and the law
- establish appropriate management and administrative practices to facilitate the sharing of police information with others
- ensure that all staff are supported in understanding their responsibilities when sharing police information. In particular, Humberside Police will support staff complying with relevant legislation and any national or local policies

3. Information Sharing Landscape

3.1 The legal circumstances relating to the sharing of police information can be summarised in three distinct groups:

- those required by or under statute (statutory obligation)
- those permitted by or under statute (statutory power)
- those made under common law to support the policing purposes including information sharing and dissemination.

Statutory Obligation

3.2 This applies where there is a specific legal obligation to disclose police information to another party. Where there is a frequent and continuing need for the Force to disclose information, a Memorandum of Understanding, a Service Level Agreement, or an Information Sharing Agreement (ISA) that clearly sets out the statutory obligations of the organisations involved, together with the procedures for managing them, should be used to ensure effective, timely and consistent disclosure.

3.3 Legislation and supporting schemes under which the police are obliged to disclose information include:

- disclosures to the Criminal Records Bureau under Part V of the Police Act 1997
- schemes to protect children and vulnerable adults
- court orders
- disclosures under the Freedom of Information Act 2000
- disclosures to data subjects under the Data Protection Act1998.

These statutory obligations are undertaken by the Information Compliance Unit, the Legal Services Unit, and other specialist units in the force.

Statutory Power

3.4 This applies where there is a specific legal power, but not an obligation, to share police information with another party.

3.5 The Police Service shares a common purpose for managing information which means that forces can share information with one another without the use of ISAs. This is often referred to as 'dissemination'. However when sharing information within the Police Service it is important that an audit trail is maintained to identify the person requesting the information and the information being shared. For the purposes of this policy the Police Service includes those forces defined in section 1 of the Police Act, 1996, the Serious Organised Crime Agency, and other forces not covered by section 1 with whom separate arrangements exist.

3.6 When the Force is requested to share information with a partner, the partner must identify a legal power that allows them to lawfully request and use such information. Examples are:

- Section 47 of the Children Act 1989 which allows local authority social services departments to request information from other agencies as part of an ongoing child protection enquiry; and
- Section 115 of the Crime and Disorder Act 1998 which gives the power to share information within Crime and Disorder Reduction Partnerships and Youth Offending Teams for crime prevention purposes.

Common Law

3.7 When the Force is asked to share information with a partner where a statutory obligation or power does not exist, a policing purpose must be established, as the decision to share is risk based and must take into account the source of the information and any restrictions on its onward dissemination. This must be balanced against the requirements of the common law duty of confidence and the DPA when personal information is shared.

3.8 In cases where the police wish to share information about sex offenders with schools or other educational establishments, *or in other circumstances where there is a pressing social need to share this type of information*, an officer of ACPO rank must approve any disclosure, balancing this with the requirements of the Human Rights Act 1998 (HRA) and the DPA. It is recognised that in extenuating circumstances, it may be impracticable to obtain the approval of an ACPO officer prior to disclosure. In this situation, the decision should be made by an officer of inspector rank or above, with reference to the template at Appendix D of this policy. Upon the disclosure of information by an officer of inspector rank or above an officer of ACPO rank must be informed as soon as practicable via liaison with Legal Services Unit.

4. Principles Governing the Sharing of Information

4.1 The decision to share information requires careful judgement in which data protection and human rights considerations are balanced with the policing purpose. Any information that the Force shares with a partner must be considered necessary for the purpose for which it is being shared.

4.2 Data Protection Act 1998

4.2.1 The Data Protection Act (DPA) provides a framework for processing (including sharing) personal or sensitive personal information. It also places a requirement on chief officers to comply with the eight Data Protection Principles. The Principles state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the data subject
- Secure
- Not transferred to other countries without adequate protection

First Principle

4.2.2 Sharing personal information fairly involves being open and transparent with the individuals whose information is to be shared. There is a requirement to inform people about the purposes of the information sharing and the agencies that will share the information, usually in the form of a Fair Processing Notice. Under some circumstances, an exemption from providing a Fair Processing Notice may apply, for

example, where the provision of this information would prejudice a current criminal investigation.

4.2.3 There is a common law duty of confidence where information of a personal or sensitive nature is collected and recorded. A breach of confidence will apply when the information collected and recorded is used in an unlawful manner.

4.2.4 Personal information disclosed by the force is likely to be sensitive in nature. Agencies that are partners in an information sharing arrangement accept that such information will not be disclosed without the consent of the individuals concerned, unless there are statutory grounds and, in the case of confidential personal information, an overriding public interest or justification to disclose.

4.2.5 When seeking information from other information sharing partners, force staff will respect the responsibility of confidentiality and will not seek to override the procedures which each agency has in place to ensure information is not disclosed illegally or inappropriately. Any conditions imposed by the recording agency should be observed.

4.2.6 Exceptions to the duty of confidence are:

- where there is a legal requirement (either under statute or a court order) to disclose the information
- where there is an overriding duty to the public (for example, where the information concerns the commission of a criminal offence or relates to life-threatening circumstances), or
- where the individual to whom the information relates has consented to the sharing.

4.2.7 In certain circumstances, consent does not need to be sought. For example, where the request to share personal information meets a policing purpose, and does not compromise operational procedures or an individual's safety. An assessment of the vulnerability of those at risk and the impact of the disclosure on the individual will need to be made before making a decision whether to seek consent.

4.2.8 The police also owe a duty of confidentiality to victims and witnesses of crime who may expect a greater level of privacy than offenders. A balance has to be struck between sharing information and the rights of victims and witnesses to privacy.

Second Principle

4.2.9 The force accepts that shared information is only to be used for a specified purpose(s). The secondary use of personal information is not permitted unless the consent of the disclosing party to that secondary use is sought and granted, having regard to the provisions of paragraph 4.2.3.

Third Principle

4.2.10 Police information must be adequate and relevant for the purpose for which it is shared. The shared information should exclude unnecessary material – for example, it may not be necessary to share details of all information held about a person.

4.2.11 The force should consider whether the purpose of sharing information can be achieved without identifying the individual(s) concerned, for example, by referring to the individual(s) using pseudonyms.

4.2.12 The force may also consider it relevant to provide a partner with information that falls outside the request. For example, information may be shared about a person who associates with an individual that may help build a more complete picture for the partner agency regarding a child's safety.

Fourth Principle

4.2.13 Information sharing partnership agencies must make every reasonable effort to ensure that the information they hold is accurate and up to date. Any inaccuracies identified must be corrected or erased as soon as reasonably practicable. Each agency should make reasonable efforts to ensure that the recipients of personal information are kept informed of changes to the personal information which they have received, so that records can be kept up to date.

Fifth Principle

4.2.14 The agencies must each comply with the various statutory timescales relating to how long particular types of information are retained. Internal procedures should be put in place to ensure compliance with this requirement. Where there are no statutory guidelines, information will be held in accordance with the fourth and fifth principles of the DPA. Police information will be assessed using the MoPI Guidelines on the Review, Retention and Disposal of Police Information.

Sixth Principle

4.2.15 The DPA gives rights to an individual in respect of their own personal information held by others. These rights include the Right of Access to

information about themselves, subject to certain exceptions, for example, where to provide certain information to an individual about themselves would prejudice a police investigation.

4.2.16 Each agency must ensure that procedures are in place to enable individuals to be given access to personal information held about them. In the case of joint records, any of the joint controlling organisations can provide access to the joint records, provided the individual is informed that the information is held jointly. Agencies in joint record holding arrangements must therefore agree to ensure they have in place procedures to enable the individual to be made aware that he/she is not obliged to apply to all of the agencies for access, and to ensure that each agency is informed that a request has been received.

Seventh Principle

4.2.17 Where information relating to an individual is shared between the agencies, each agency must take reasonable steps to ensure this information is transferred in a secure manner. Appropriate measures must be taken to ensure that data is stored and held in a secure manner. These measures will ensure that access to the information can only be obtained by those with the need and the right to know.

4.2.18 All information, particularly personal or sensitive data, must be allocated an appropriate protective marking, under the Government Protective Marking Scheme (GPMS). Depending on the degree of sensitivity involved, information should be marked RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. In practice, most personal or sensitive information will be marked RESTRICTED. Please refer to the Practice Direction on GPMS.

4.2.19 Agencies should seek to ensure their management of information security meets the standards set out in ISO 27001.

Eighth Principle

4.2.20 Wherever sharing information outside the European Economic Area (EEA) is considered, contact the Information Compliance Unit for guidance.

4.3 Proportionality

4.3.1 When considering whether to share personal information there is a need to ensure a fair balance between the protection of an individual's rights and the general interests of society.

4.3.2 Sharing personal information will be proportionate if:

- the individual concerned consents to the information being shared, or
- the purpose justifies infringing the right to privacy and
- the measures taken to meet the purpose are rational and fair and
- the means used to share are no more than is necessary to accomplish the purpose.

4.3.3 The threshold test of proportionality is lower when sharing factual information, but higher about less serious crimes as there is a lower public interest in the exchange of this information. This means that a case-by-case decision needs to be made that the information sharing is in the public interest, is proportionate, and any infringement of an individual's rights under the HRA is necessary.

5 Information Sharing Agreements

5.1 Information Sharing Agreements (ISAs) are formal agreements between organisations who wish to share personal information. ISAs must be held and managed centrally within the Force. These agreements are intended to cater for long term information sharing rather than those occasions when personal information is required to be shared on a 'one-off' basis.

5.2 An ISA provides a framework to facilitate confidence in information sharing. It should not be viewed as a bureaucratic obstacle to be overcome before any information sharing can take place. For example, where the police are involved in a partnership arrangement with another agency, it would normally be appropriate for an ISA to be in place, but individuals working within the partnership (such as a police officer within a local authority) should not feel constrained to fill in a form every time they speak to a colleague.

5.3 The Advantages of ISAs

5.3.1 ISAs should be established and applied between the Force and its partners in line with this Force policy. The particular advantages of ISAs are that they:

- ensure consistency in the way information is shared
- allow the force to place conditions on the way information will be handled by the partner agency and vice versa
- ensure that information can be shared lawfully
- can help to build confidence in the role that the police play in protecting the public.

5.4 The Process of Developing an ISA

5.4.1 It is important to remember that the creation of an ISA does not in itself make information sharing or disclosure lawful. Each agreement must clearly identify the legal basis for any disclosure activity. Even when an ISA is agreed the basic rules of disclosure must still be followed, as specified in Section 4 of this policy.

5.4.2 It is only lawful to share information either under a legal power (e.g. Section 115 Crime and Disorder Act 1998), or for a policing purpose, i.e:

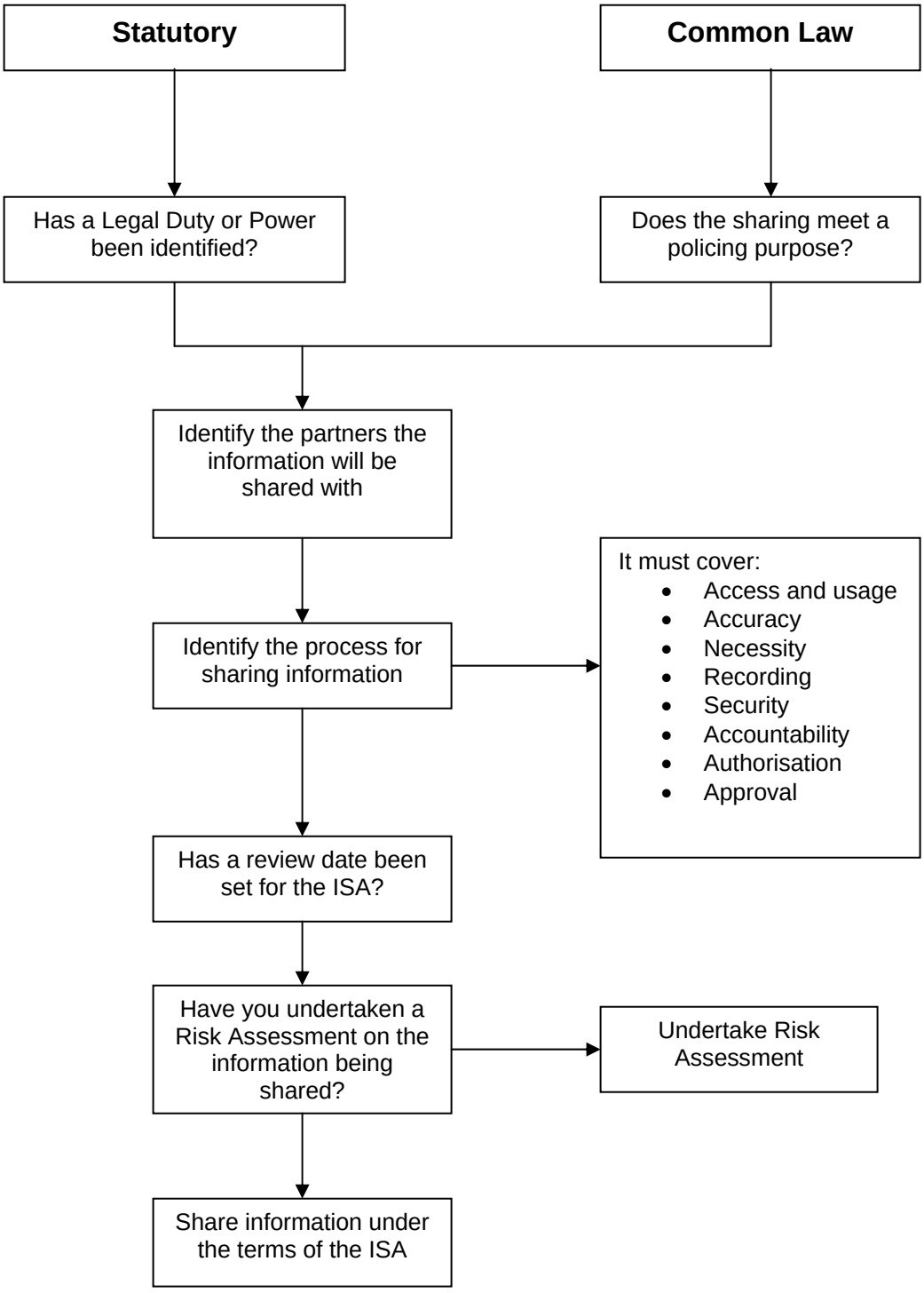
- protecting life and property
- preserving order
- preventing the commission of offences;
- bringing offenders to justice
- any duty or responsibility arising from common law or statute.

5.4.3 Details of the partner agencies together with names, addresses and contact details must be recorded on the agreement. Identifying partners helps to confirm whether the partner can rely on a statutory purpose to request information or whether the decision to share is based on common law and, therefore, requires a policing purpose to be established.

5.4.4 The process for sharing information should be set out in the agreement. This will provide those involved with a clear understanding of how the information will be shared, to whom and when. It is also an opportunity for conditions to be placed on how the information may be used. A list of questions which should be asked when developing an ISA is included at Appendix A. Providing these questions have been answered, are clearly explained in the document and recorded, then information sharing can take place.

5.5 The flowchart at figure 1 below depicts the process for developing an ISA.

Figure 1: The ISA process



5.6 A blank ISA template (Appendix B) is included at the end of this document. The ISA template may be copied and used in the development and use of ISAs. All ISAs developed by Humberside Police must comply with the ISA template and sited in the ISA central repository.

5.7 **Authorisation to develop an ISA**

5.7.1 The development of an ISA for a specific information sharing requirement must be authorised by the Divisional Commander in the relevant business area(s). The developed ISA should be referred for quality assurance to the Head of the Information Compliance Unit, who will approve the ISA on behalf of the Chief Constable.

5.8 **Review**

5.8.1 Undertaking reviews to ensure that an ISA is achieving its purpose and the actual process of sharing is operating smoothly is an integral and essential part of the agreement.

5.8.2 Reviews will be undertaken jointly by the Head of the Information Compliance Unit, relevant business area and partner agency where appropriate.

5.8.3 Reviews will be 6 months after the ISA's commencement and then annually or every two years subject to Risk Assessment.

5.8.4 A checklist of the stages to be covered in the review process is included at Appendix C.

6 Sharing police information outside an ISA

6.1 Where an Information Sharing Agreement does not exist, or the decision to share is a one-off**, and there is a pressing need to disclose,** the template at Appendix D must be completed, risk assessed on a case by case basis and the decision to disclose or not to disclose, must be documented before any sharing of police information takes place. This risk assessment process must be recorded, and the officer concerned must ensure that they have the authority to make such a disclosure. Upon the disclosure of information outside an ISA Legal Services Unit must be informed as soon as practicable.

7 Responsibilities for managing information sharing

7.1 Head of Information Compliance Unit

- Quality monitoring of proposed ISAs;
- Providing professional advice and guidance to staff developing new ISAs;
- Approving ISAs on behalf of the Chief Constable;
- Maintaining a central database of all force ISAs.

7.2 Managers:

- Supporting staff to share information appropriately;
- Ensuring all ISAs are held and managed centrally within force;
- Ensuring that the process of sharing information is adhered to by both supervisors and users;
- Authorising ISAs, ensuring compliance with the ISA template;
- Ensuring that ISAs are reviewed in accordance with force policy;
- Ensuring that staff who have a responsibility for sharing information are trained in accordance with the National Training and Delivery Strategy.

7.3 Supervisors:

- Supporting staff to share information appropriately;
- Auditing, on an ad hoc basis, the decision to share made by users, including the necessity, accuracy, adequacy and relevance of the information shared;
- Checking whether the decision to share meets a policing purpose or is based on a specific legal duty or power;
- Taking reasonable steps to ensure that the information being shared does not compromise any police operation or the safety of others;
- Ensuring that a risk-assessment process is adhered to by the user when making a decision to share information;
- Providing feedback to staff on their performance.

7.4 Users:

- Ensuring that the information being shared meets a policing purpose or is lawfully disclosable for a statutory purpose and is proportionate and necessary;
- Ensuring that the information is relevant, accurate and adequate for the purpose for which it is being shared;

- Ensuring that when the personal information is shared, the requirements of the Data Protection Act 1998 and the common law duty of confidence have been fulfilled;
- Applying a protective marking to the information being shared under the Government Protective Marking Scheme, where applicable;
- Carrying out a risk assessment where information is shared with partners in the voluntary or private sectors who do not have a statutory purpose to share information;

8 HUMAN RIGHTS

8.1 Any action taken under the provisions of this Practice Direction will be proportionate, necessary and justifiable.

8.2 Actions taken under the provisions of this PD could be subject to scrutiny in Civil Courts. In addition any person aggrieved by any action taken can make use of the complaints procedure.

8.3 This PD is suitable for publication to the general public.

8.4 This PD will be subject to review every three years or sooner in the case of a change in policy or legislation.

9. RACE EQUALITY SCHEME

9.1 The content of this PD has been considered under the provisions of the Race Equality Scheme, as dictated by the Race Relations Act 1976 (as amended) and the Race Relations Amendment Act 2000, and deemed to be non-relevant.

10. EQUALITY IMPACT ASSESSMENT

10.1 An Equality Impact Assessment has been undertaken covering Diversity, Race, Disability, Gender, Sexual Orientation, Religion and Beliefs and Age.

Policy Information

Policy Owner:	Head of Information Compliance Unit
Reviewed for compliance with Human Rights Act 1998	Reviewed by: Inspector Shimells Date: 12 June 2008
Reviewed for compliance with Race Relations (Amendment) Act 2000	Reviewed by: Inspector Shimells Date: 12 June 2008
Diversity Impact Assessment carried out	Assessor: Inspector Shimells Date: 12 June 2008
Effective Commencement	Date: 8 July 2008
Last Reviewed	Date: 8 July 2008
Next Scheduled Review due (6 months after commencement/ 12 months since last review date	Date: 8 January 2009

APPENDIX A

Questions to be asked when developing an Information Sharing Agreement (ISA)

1. What information is to be shared?

   Any information being shared must be proportionate and necessary for the purpose for which it is being shared. The type of information may need to be defined, e.g. convictions, cautions, names, addresses, as may its location.

2. Is there an existing ISA that satisfies this information sharing requirement?

   There may be other ISAs in place that cover the same information sharing process. If the same process is in place with other partners, the ISA(s) could be adapted to meet the current requirement. Check the Information Compliance Unit website for existing ISAs.

3. Who will have access to the information and what may they use it for?

   Who or which business areas within the partner agency will have access to the shared information?
   What vetting or confidentiality agreements does the partner agency have in place to counter the possibility that sensitive information may be compromised?
   How will the information be securely stored?
   If the partner agency does not conform to the Government Protective Marking Scheme (GPMS) the decision as to who has access and what they may use it for is risk based.

4. How will the information being shared be kept accurate and up to date?

   The force is responsible for ensuring that any information it shares is accurate and current.

5. How long a period will the information be retained for?

   The ISA can be used to specify when the information the partner received should be reviewed and subsequently retained or disposed of. This must be in line with the force review, retention and disposal policy.

6. How is the security of the information being shared ensured?

   The ISA can, where applicable, be used to apply a protective marking to the information being shared in line with the GPMS. There may also be a need to apply other safeguards in relation to the transit or storage at a

partner site. All parties must agree to keep all relevant data secure and comply with the Data Protection Act.

7. Who is accountable for the ISA?

Every individual involved in drafting an ISA has a responsibility to ensure that the information being shared is processed on compliance with the law and with national standards. The names of the individuals responsible for the development of the ISA within the force and partner agencies should be clearly stated on the file.

8. Who will approve and authorise an ISA?

Once the ISA has been finalised, the force and partner agencies must ensure that they fully understand and agree with the purpose, process and conditions of the agreement. It will be the responsibility of the business area owner to agree the ISA which will be approved on behalf of the Chief Constable by the Head of the Information Compliance Unit. In partner agencies, the signatory should also be a senior member of staff who can be held accountable for the processing of information.

9. How will compliance with the Data Protection Act 1998 be ensured if the information shared is personal or sensitive personal information?

Whenever personal information is held by a partner organisation, it must be processed in accordance with the eight principles of the Data Protection Act.

10. Where will the ISA be held?

All ISAs must be held centrally and made available to all staff on the force intranet. A high level summary of the agreement can be added that provides a brief description of the purpose, partners and process together with the name of the individual who is tasked with maintaining the agreement. Where possible, ISAs should be made publicly available.

Appendix B

GENERIC TEMPLATE FOR INFORMATION SHARING AGREEMENTS AND PROTOCOLS

November 2007

INTRODUCTION

A Code of Practice on the Management of Police Information (MoPI) was introduced under the Police Act 1996 and Police Act 1997, following the Bichard Inquiry into the 2002 'Soham Murders'.

Guidance has been issued under this Code which relates to the development of Information Sharing Agreements (ISAs). The national Action Plan to implement the Guidance requires each Force to use one template upon which every ISA must be based.

From *(date)*, no ISA may commence unless it complies with the attached template. Existing ISAs/protocols should be converted into the template format by *(date)*.

PURPOSE OF THE TEMPLATE

Information Sharing Agreements (ISAs) should be used when the police request or are requested to share information with others on a regular and ongoing basis.

An ISA provides a framework to facilitate confidence in information sharing. It should not be seen as a bureaucratic obstacle to overcome before any information sharing can take place.

The template will enable you to produce a robust agreement that meets all legal requirements and achieves the desired partnership outcomes, whilst at the same time meeting the requirements of MoPI, the Humberside Police Information Sharing Policy, and the ACPO Common Security Policy.

In fact using the template before you start negotiating an agreement will enable you to determine: whether an agreement is beneficial to Humberside Police; whether it is in the public's interest; and the issues you need to explore before developing the agreement.

MoPI introduces requirements to fully document the process of information sharing – including the rationale behind what is to be shared, how it is to be shared, with whom etc. It introduces requirements to review and audit ISAs. The Data Protection Act 1998 (DPA) requires those sharing information to satisfy each of the eight principles underpinning the Act. To safeguard the interests of Humberside Police, it is necessary to ensure that the manner in which these principles are satisfied is fully documented.

This template provides direction or guidance within a number of sections to ensure all the above requirements are met whilst minimising the amount of detailed knowledge required in writing an ISA.

USE OF THE TEMPLATE

The template provides mandatory sections and sub-sections (titled) which are to be used, in the order specified, in drafting any ISA.

The template comprises text in **black** font colour and text in **blue** font colour.

That text which is in black is mandatory and must be used. Section headings (1 to 13) are also mandatory.

The use of sub-section titles (e.g. 4.1, 4.2 etc) is not mandatory, **but** it is mandatory to include relevant text at that part of the agreement (i.e. paragraph numbering can be used within the section rather than sub-sections if required).

That text which is in **blue** is explanatory text that usually describes what sort of information the template user must or should detail within that section of the template, i.e. the agreement must include text that addresses the issue or point raised.

Blue text also provides examples by way of illustration and general guidance.

Once an agreement reaches a final draft form it should be circulated to the Information Compliance Unit and the Legal Services Unit for their specialist opinion. *(nb this procedure is to be decided)*

Once ratified, an electronic version of the agreement should be sent to the Information Compliance Unit at Headquarters to be included on the Force Intranet.

1. INTRODUCTION

This agreement has been developed to:

- Document the specific purposes for which the signatory partners have agreed to share information.

- Describe the roles and structures that will support the exchange of information between partners.

- Set out the legal gateway through which the information is shared, including any reference to the DPA, the Human Rights Act 1998 (HRA) and the Common Law duty of confidentiality

- Describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities including under the DPA and any partner specific security requirements.

- Ensure compliance with individual partners' policies, legal duties and obligations.

- Ensure that Humberside Police complies with the Code of Practice on the Management of Police Information made under the Police Act 1996 and the Police Act 1997.

- (N.B. Add any additional requirement which may be specific to this particular agreement)

2. PURPOSE AND SCOPE OF THIS AGREEMENT

This section should provide a high level summary of the agreement and a brief description of the purpose and scope of the agreement. This should be detailed enough to give someone unfamiliar with the agreement a clear understanding of what it is about in general terms.

For instance this may be as brief as: 'The purpose of this agreement is to facilitate the exchange of information pursuant to the power contained in section 115 of the Crime and Disorder Act 1998 to disclose information to relevant authorities within the Kingston upon Hull Crime and Disorder Partnership to meet the partnership aims in respect of Child Safety Orders, removal of truants, and the reduction of crime and disorder in and around schools'.

3. BENEFITS OF SHARING THIS INFORMATION

Detail how this agreement will benefit the general public or a section of it. This might relate to actual or potential victims of crime; or a more general public

interest including a reduction in any behaviour being targeted by a Crime and Disorder Partnership.

Detail here the benefits to each partner individually or collectively. For instance, explain how the information sharing partnership helps achieve any obligations or duties that Humberside Police or its partners have.

The benefits listed above must be directly attributable to the information sharing and must be sufficiently detailed to make sense to someone unfamiliar with the agreement (but who has read the summary above). The benefits to the community will be particularly key to determining whether the agreement can satisfy the legal requirements for information sharing in the public sector, especially where a common law duty of confidence exists.

Individuals should only be identified where this is necessary to achieve the purpose(s) of the information sharing, otherwise anonymised or statistical information should be used.

4. AGREEMENT ADMINISTRATION

4.1. Partners to the agreement

List here all the partners involved in delivering this particular agreement. This should include the name of the organisation and the address to which any correspondence should be sent.

4.2. Commencement of the agreement

This section should formally record when the agreement is deemed effective from, e.g. 'This agreement shall commence upon the signing of a copy of the agreement by the partners'; or a particular date should be inserted if this is preferable.

4.3. Withdrawal from the agreement

Any partner may withdraw from this agreement upon giving written notice to the other signatories. The partner must continue to comply with the terms of this agreement in respect of any information that the partner has obtained through being a signatory. Information which is no longer relevant should be returned or destroyed in an appropriate manner.

4.4. Review of the agreement

In accordance with the requirements of the Code of Practice for the Management of Police Information, this Agreement will be reviewed six months after its implementation and subject to Risk Assessment annually or every two years thereafter.

The review will:

- Ensure the contact list is up-to-date.
- Consider whether the agreement is still useful and fit for purpose.
- Identify any emerging issues.
- Determine whether the agreement should be extended for a further period (up to one year) or whether to terminate it.

The decision to extend or terminate the agreement, and the reasons, will be recorded. *(NB need to develop a template for this)*

4.5. Audit Arrangements

As part of the requirements of the Code of Practice for the Management of Police Information, the single point of contact (SPOC) identified by Humberside Police will maintain an Information Sharing File in respect of this agreement.

This file (which may be electronic or paper based) will contain:

- Record of Humberside Police information disclosed
- Record of information disclosed to Humberside Police
- Decision or justification to disclose or not disclose
- Access and vetting list
- Notes of meetings with partners
- Details of recent correspondence and phone calls
- Record of any review of the agreement
- Add any additional requirements.

Other partners to this Agreement are responsible for maintaining their own procedures to ensure any information sharing is recorded and documented in accordance with their business needs.

Detail any procedures to be put in place to ensure that any information sharing is recorded and documented by each of the other partners.

5. POWER OR DUTY TO SHARE INFORMATION

It is necessary that the sharing of information is in accordance with a statutory power or that it is permitted under common law to support a policing purpose.

In this section, the relevant statutory power or policing purpose that provides the legal framework under which the information is to be shared must be listed. In some cases this may be an implied power.

Some examples of the legal framework for sharing information within an agreement are:-

- To meet one or more of the policing purposes:
  - protecting life and property

    - preserving order
    - preventing the commission of offences
    - bringing offenders to justice
    - fulfilling a duty or responsibility arising from common law or statute
- Section 115 Crime and Disorder Act 1998
- Section 120 Learning and Skills Act 2000
- Section 11 Children Act 2004
- Section 135 Housing Act 1996
- Anti-Social Behaviour Act 2003
- Section 47 Children Act 1989

This is not an exhaustive list – consult the Information Compliance Unit and/or Legal Services Unit for guidance if necessary.

6. LEGAL COMPLIANCE

Once completed this section will ensure relevant provisions of the DPA, the HRA and any Common Law duties have been met

6.1. Overriding any duty of confidence

There are circumstances where an obligation of confidence arises and to breach that confidence without reasonable justification could give rise to a complaint and may contravene the DPA.

Information is likely to have been considered as having been provided in confidence where the purpose of sharing is not in line with the likely expectation of the person who originally provided that information. For example, a witness to a crime who contacts the police would not ordinarily expect their details to be provided to anyone not involved in investigating or prosecuting the offence.

Exemptions from this duty of confidence are:

- The individual to whom the information relates has consented to the sharing of the information, or
- The information sharing is required by law.

In this section either:

- **State** 'This agreement does not relate to any information where a duty of confidence exists', **or**
- **Explain** how one of the two exemptions applies.

In particular, if relying on the consent of individuals, state how the consent is obtained and recorded – consent must be specific, informed and freely given, and capable of being withdrawn. Consent is not genuine unless its withdrawal leads to the information sharing being stopped.

6.2. Necessity of the information sharing

This section applies only where 'personal data' (as defined by the DPA) is to be shared. If no such data is to be shared, simply insert 'This Agreement does not relate to personal data.' This would apply, for example, where the purposes of the information sharing can be achieved without identifying specific individuals.

Whilst section 3 explains the benefits to be achieved as a result of the information sharing, the DPA requires that the sharing of the information in the manner proposed meets certain tests of necessity.

The necessity may arise to comply with a legal obligation, exercise a function under a statute, or for the purposes of the legitimate interests pursued by the signatory partners (including a policing purpose).

Explain in this section the legal obligation, statutory function or legitimate interest that the sharing of information within this agreement seeks to meet.

An example could be, 'Humberside Police exists to prevent and detect crime and Grimsby Businesses against Crime (GBAC) comprises retailers who sell to the public. The exchange of this information will enable the prevention and detection of theft and violent offences affecting the Grimsby Town Centre area. This will be achieved because security personnel will be able to identify those with previous offending behaviour and take appropriate measures – including the provision of criminal intelligence to Humberside Police'.

6.3. Fair processing of the information

This section applies only where 'personal data' (as defined by the DPA) is to be shared. If no such data is to be shared, simply insert 'This Agreement does not relate to personal data.'

SEEK THE ADVICE OF THE INFORMATION COMPLIANCE UNIT IF NECESSARY BEFORE COMPLETING THIS SECTION.

The DPA requires the fair processing of information unless an exemption applies. In particular, fairness involves being open with people about how their information is used. The most likely exemption from the fairness requirement is sharing personal information for the prevention and detection of crime, apprehension or prosecution of an offender without the individual's knowledge, where disclosure of that fact would be likely to prejudice the investigation.

In this section state how the information will be processed fairly by informing individuals about the purposes of sharing their information and who it will be shared with, or explain how complying with the fair processing requirements would be likely to prejudice the purposes of the agreement.

6.4. Justification for the provision of sensitive personal information

Sensitive personal information is information about an individual which relates to:

- the commission or alleged commission of an offence;
- proceedings relating to an offence;
- physical health, mental health or sex life;
- race, ethnic origin or religious belief; or
- political opinions or trade union membership.

The majority of information that Humberside Police seeks to share with its partners contains 'sensitive' personal information. This section will therefore apply in most circumstances. The DPA requires that one or more conditions must be satisfied before 'sensitive' personal information can be shared.

Where the information intended for sharing is not 'sensitive', simply **state** – 'No sensitive personal information is subject to sharing for the purposes of this Agreement'.

IF THE INFORMATION IS 'SENSITIVE' MATERIAL AS DESCRIBED ABOVE; REFER TO THE INFORMATION COMPLIANCE UNIT.

The list below, which is not exhaustive, details some of the DPA conditions that might enable 'sensitive' personal information to be shared. At least one condition must be recorded.

- The sharing of the information is necessary for (a) the administration of justice, (b) for the exercise of any functions conferred on any person (including a constable) by or under an enactment, or (c) for the exercise of any functions of the Crown, or a government department

- The sharing of the information is necessary for the exercise of any functions conferred on a constable by any rule of law.

6.5. Proportionality

Those partners to this agreement which are public authorities are satisfied that the nature of the information to be shared under this agreement and the manner of such sharing is compatible with the requirements of the HRA, having particular regard to the exemptions to the right to respect of family life set out within Article 8(2) of the HRA.

The remainder of this section applies only where 'personal data' (as defined by the DPA) is to be shared. If no such data is to be shared, simply insert 'This Agreement does not relate to personal data.'

Detail how the sharing of information of the type described in Section 7 is in pursuit of a legitimate aim, proportionate, appropriate and necessary to a

democratic society. This may relate to the beneficial effects of the information sharing to the majority of citizens if these have been set out earlier within section 3 of this agreement.

7. TYPES OF INFORMATION TO BE SHARED

This agreement has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case. Any information being shared must be proportionate and necessary for the purpose for which it is being shared.

Information will not be shared where disclosure would prejudice ongoing proceedings or sensitive cases unless there is an overriding public safety requirement to do so.

The agreement will need to set out the type of information which may be shared under this agreement. This could include details of individuals, convictions, cautions or other information. It may also be necessary to identify where the information is kept.

Provide *specific* details of the information that will be supplied by each partner (listed under each partner). These details should enable a practitioner to easily determine exactly what information can be shared.

For example, within the agreement, the type of information to be shared may state:

'Humberside Police will share:

> In respect of persons who have, within the previous twelve month period, been subject to a conviction, caution, final warning, reprimand or fixed penalty notice for theft, violence or disorderly behaviour in the vicinity of Grimsby town centre (or are the subject of an Anti-Social Behaviour Order for such behaviour), the photograph, full name, date of birth, physical description, PNC warning markers or Intelligence System information regarding possession of weapons or use of violence - this information being made available to all signatory partners.

Grimsby Businesses Against Crime will share:

> Evidence, including complaints from the public relating to criminal or anti-social behaviour at, or in the immediate vicinity of, Grimsby Shopping Mall, which relate to a person whose photograph and details have been circulated by Humberside Police under this agreement - this will include details of associates and vehicles recorded by Mall staff.'

8. ROLES AND RESPONSIBILITIES

This section should detail the intended recipients of the information, arrangements for training and awareness, dispute resolution procedures, single points of contact, maintenance arrangements, contact details etc.

8.1. Single Point of Contact (SPOC)

Each partner will appoint a SPOC who will be a manager of sufficient standing and who will have a co-ordinating and authorising role. A partner may also appoint a supervisor or manager to deputise for the SPOC.

The following named individuals are the SPOCs, or Deputies, for the partner organisations who will be responsible for data protection, security and confidentiality, and compliance with all relevant legislation.

NAME	POST	ORGANISATION
[Insert name]	[Insert position]	[Insert name of party]
[Insert name]	[Insert position]	[Insert name of party]
[Insert name]	[Insert position]	[Insert name of party]

The specific responsibilities of the above are:

- Making sure the named party abides by this agreement
- Ensuring relevant staff are fully aware of their responsibilities
- Appointing other staff to act in their absence
- Controlling the release of the information and maintaining its integrity
- Deciding on a case by case basis if and why a public interest overrides a duty of confidence
- Keeping an information sharing file (or similar), which holds all the partner's information sharing documents in general
- Ensuring any changes to the SPOC are confirmed in writing
- Add any other responsibilities.

The appointment of a SPOC helps to ensure that specific arrangements work as efficiently as possible and also has the benefit of improved communication between partners, particularly if they have a named person to contact.

Whilst some agreements will set out the criteria for sharing information; in relation to personal data, an assessment will be required on a case by case basis. The Crime and Disorder Reduction Partnerships are good examples where such assessments are required and where a **Designated Officer** should be appointed to manage the flow of information.

If appropriate a term other than single point of contact/designated officer may be used as long as the responsibilities are made clear.

9. PROCESS OF SHARING

The information may only be used for the purpose/s set out in this Agreement.

Partners to this agreement will respond to any notice from the Information Commissioner that imposes requirements to change the way in which personal data is processed or to cease processing personal data.

9.1. Access to the information

Detail here the individuals or business areas within partner agencies that will have access to the shared information, particularly if it is information that may compromise an operation or place an individual at risk.

Detail here the vetting or confidentiality arrangements Humberside Police or another partner wishes to impose.

9.2. Sharing procedure

This section should detail the process for requesting information; how the information will be transferred between partners; the source of the information and, where appropriate, how the information will be extracted (including editing or removal of third party details), e.g. name and address fields exported to CD by Humberside Police personnel.

This section should refer to the **mandatory appendix 1** (which details a checklist/flow chart for practitioners), **mandatory appendix 2** (which details sharing outside of the agreement) and any additional appendix which contains forms to request or provide information.

9.3. Ensuring the accuracy of information shared

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made

Humberside Police and individual partners are responsible for ensuring that any information they share is accurate and, where necessary, kept up to date. **Detail** the arrangements to ensure compliance with this requirement.

9.4. Review, retention and disposal

Detail agreement specific review, retention and disposal requirements and how the information will be disposed of confidentially (e.g. by use of cross-cut shredding machines or return to the original sharing partner).

9.5. Security of the information being shared

The information must be stored securely and destroyed when it is no longer required for the purpose for which it is provided.

It is expected that partners to this agreement will have in place baseline security measures compliant with BS17799:2005 and ISO/IEC 27001:2005, and HMG standards in relation to information security. Only nominated representatives can access, request information, and make disclosure decisions. Data should be stored securely to prevent unauthorised access and disclosure

Each party agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the DPA to the data, e.g. make accidental compromise, loss or damage unlikely during storage, handling, use, processing, communication, transmission or transport; deter deliberate compromise or opportunist attack, and promote discretion in order to avoid unauthorised access

The Information Security Officer from Humberside Police will, by arrangement, undertake a physical review of the security in place to ensure the confidentiality, integrity, availability and non-repudiation of the Force information being stored under this agreement.

The information shared must not be disclosed to any third party without the written consent of the partner that provided the information; unless it is disclosed under a statutory obligation or by Humberside Police for a policing purpose.
(There may be other overriding public interest considerations peculiar to a partner, other than Humberside Police - these considerations may be additionally listed).

THE ADVICE OF THE INFORMATION COMPLIANCE UNIT SHOULD BE SOUGHT WHEN WRITING THIS SECTION OF THE AGREEMENT.

The agreement can be used to apply a protective marking to the information being shared in line with Humberside Police policy, where applicable. Where Humberside Police shares information with others who do not recognise Protective Marking, the decision as to who has access and what they may use it for, is a risk-based decision.

Detail here how the information will be transferred to and stored by the partners, and the physical security arrangements; whether information will be processed on a partner's system and if so, the security arrangements in place; how security incidents will be notified to the relevant partners, etc.

10. MISCELLANEOUS MATTERS

This should detail any miscellaneous administrative matters not captured adequately elsewhere.

10.1. Indemnity

Partners to this agreement are aware that the deliberate or reckless disclosure of personal data (obtained under this agreement) to other organisations or persons may amount to a criminal offence under section 55 of the DPA.

Partners to this agreement indemnify Humberside Police (to include the Chief Constable his officers and staff and the Police Authority) against any costs, damages and expenses it incurs in connection with and arising from legal claims (of whatever nature) against Humberside Police arising from this Agreement, to include, but not limited to, claims arising from an alleged breach of this agreement, misuse of the information or wrongful disclosure by the Partner and breach of confidentiality, save where the claim arises directly and solely because of the negligence of Humberside Police.

It is the opinion of the Humberside Police Legal Department that the above paragraph should be included within all ISAs. The paragraph will therefore be included UNLESS an exceptional reason exists not to do so.

In such a case the reason must be documented in the Information Sharing File and approved by an officer not below the rank of Superintendent.

10.2. Access Rights of data subjects

If a party to this agreement receives a subject access application under section 7 of the DPA and personal data is identified as belonging to another signatory partner or a third party, it will be the responsibility of the receiving agency to contact the data owner to determine whether the latter wishes to rely on the right to any statutory exemption under the provisions of the DPA. Where the information cannot be provided without disclosing information relating to another individual who can be identified from that information, there is no obligation to comply with the request unless the other individual has consented to the disclosure of the information to the person making the request, or it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual
- any steps taken by the data controller with a view to seeking the consent of the other individual
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

10.3. Freedom of Information Act Considerations

If a party receives a request for information under the Freedom of Information Act 2000 and the information requested is identified as belonging to another

Organisation, it will be the responsibility of the receiving agency to contact the data owner to determine whether the latter wishes to rely on any statutory exemption under the provisions of the Freedom of Information Act and to identify any perceived harm.

Unless an exemption is stated below Humberside Police will make this agreement available under its Freedom of Information Act publication scheme.

Detail any such exemption or state 'This Agreement will be made available under the Freedom of Information publication scheme operated by Humberside Police' (and any other named partner who is a public authority).

Where some of the detail of the agreement may be subject to an exemption under the Act it will be useful if this detail is recorded in an appendix to enable disclosure of the entire agreement excluding that appendix.

If required, seek the advice of the Information Compliance Unit.

11. SIGNATURES

By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement.

Signatories must also ensure that they comply with all relevant legislation.

Signed on behalf of ……:

.....

Title: .....

Position: .....

Date: .....

Signed on behalf of Humberside Police:

.....

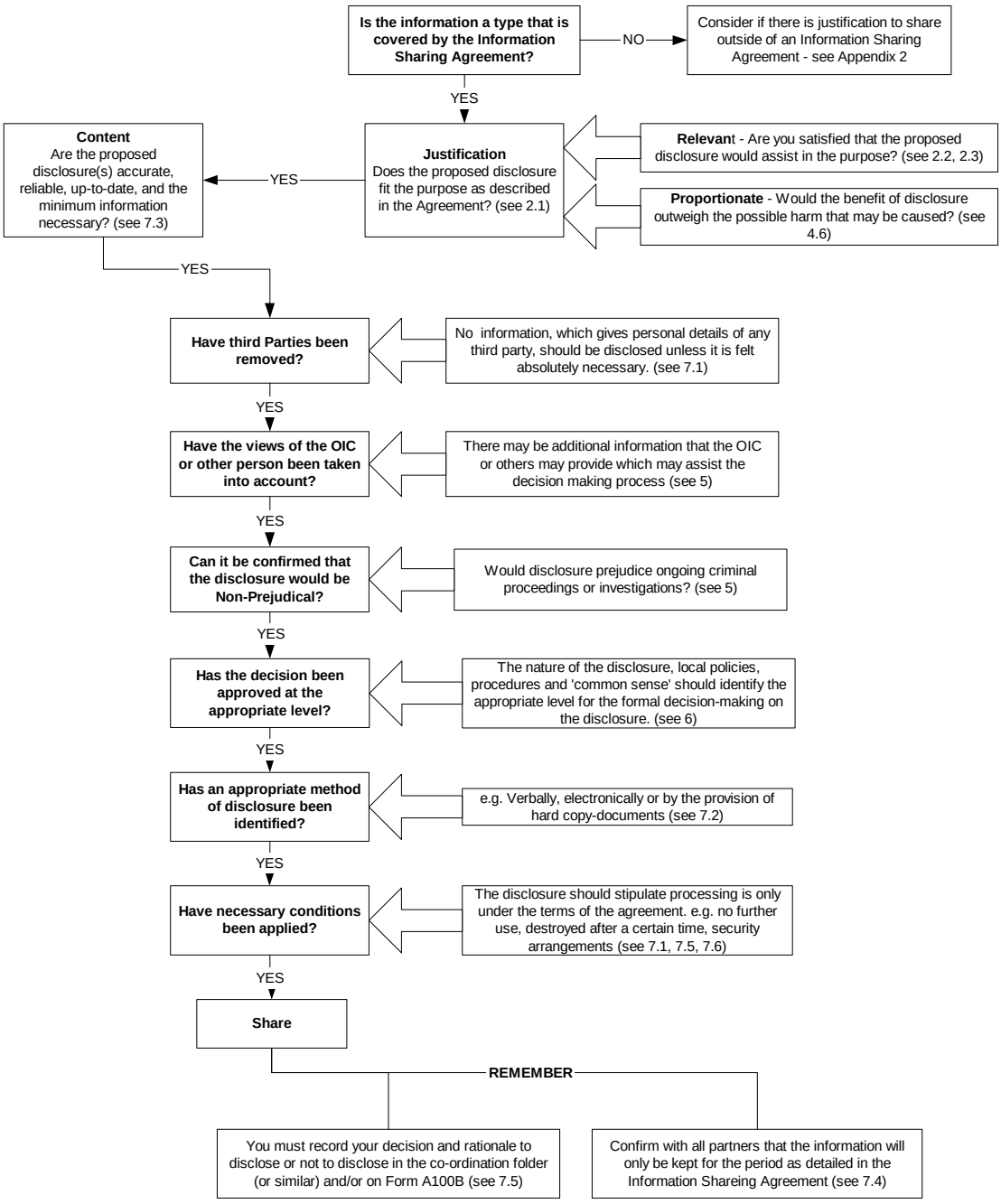
Title: .....

Position: .....

Date: .....

12. APPENDIX 1 – Decision Making Filter

This filter is designed to assist decision makers in determining, on a case by case basis, whether information of a particular type can be shared under the auspices of the information sharing agreement (ISA).



13. APPENDIX 2 – Sharing Outside of the Agreement

Template for completion where an Information Sharing Agreement does not exist, or the decision to share is a one-off **and there is a pressing need to disclose**.

Considerations & Key Questions	**Response**
Do you have the authority to make this disclosure?	
Is there a pressing need to disclose? Document this.	
Identify who is asking for the information.	
Record the name, position, organisation and contact details of the enquirer.	
How have you verified the identity of the person requesting the information?	
Is there an agreement already in place which will meet the need? If yes, use the current ISA	
Record what information is being asked for. Is it the minimum required for the purpose? What purpose will it be used for? Is it a policing purpose?	
What is the legal basis or policing purpose to support the sharing of information.	
Has written consent of the individual(s), to whom the disclosure relates, been provided? If not, record reason why not? If victim/witness information requested, have they been given the opportunity to consent/refuse? If not, record why not? Is there a pressing need for the victim/witness information as well; is it relevant? If so record.	
Is the enquirer requesting personal information? Would de-personalised information suffice?	
Is the information requested proportional and relevant to the purpose for which it is required?	
Is there an equally effective but less intrusive alternative method of achieving the aim? If so what?	
Can the objective(s) of the information sharing be achieved without identifying the individual(s) concerned?	
Is there time to put the request in writing? Fax it, for example? If not why not?	
When do they want the information and how do they want it communicated? Is it a secure method? If not, do the risks of not disclosing outweigh the risks of insecure communication? Document these.	
What is the vulnerability and likely impact on the subject of the disclosure? What is the likely impact of not disclosing? Does the risk of disclosing outweigh the risk of not disclosing? Document this.	
Record the decision to disclose or not to disclose.	
Record what information was shared (or not shared) - attach to this completed template if more space is required.	
Is this likely to be a regular request? If so an agreement must be drafted and agreed for future use.	
Name of person making disclosure with details of any	

authorising person.	
Date:	

This template must be completed, risk assessed on a case by case basis and documented, before any sharing of police information takes place. This should be retained securely in accordance with the Force retention policy. Contact the Information Compliance Unit for advice if necessary.

Appendix C

Stages to be covered in the Review Process

1. Is the contact list correct?

   Each signatory organisation has a responsibility to maintain up-to-date contact details of the key individuals operating or managing the sharing activity. When a change in personnel occurs, the partner in question should ensure that the other partners are aware of the change and adjust the ISA accordingly.

2. Is the ISA still useful and fit for purpose?

   If the partners decide that the ISA is no longer useful it should be terminated.
   This is also an opportunity to ensure that the correct information is being shared and that the ISA does not need to be adjusted to reflect any change in needs. Where a change is required this must be agreed by the partner agencies, and an addendum made to the ISA, indicating the reasons for the change(s). This will form part of the audit trail. If substantial amendments are required then a new ISA may be necessary.

3. Has the review identified any emerging issues?

   The review provides an opportunity to discuss any problems that may have arisen. Reviewers will also need to be aware of any changes in legislation that may impact on the ISA.
   Reviews can also be used to identify any gaps in the information sharing regime and identify requirements for other ISAs.

4. Are procedures for ensuring the quality of information being adhered to and are they working in practice?

   The review should identify if any of the information sharing partners are failing to meet agreed standards in areas such as accuracy of information, data retention, information security, etc.

5. Are the provisions for guaranteeing individuals' DP rights adequate?

   The review should highlight the accuracy and continuing relevance of Fair Processing Notices, and the effectiveness of procedures for dealing with Subject Access Requests.

6. Extending / terminating the agreement.

At the end of the review, a decision should be made on whether to extend the ISA for a further period (typically 1 year) or whether to terminate it. Any decision should be recorded with the reasons for choosing a particular course of action clearly stated.

Appendix D

Template for completion where an Information Sharing Agreement does not exist, or the decision to share is a one-off **and there is a pressing need to disclose**.

Considerations & Key Questions	**Response**
Do you have the authority to make this disclosure?	
Is there a pressing need to disclose? Document this.	
Identify who is asking for the information.	
Record the name, position, organisation and contact details of the enquirer.	
How have you verified the identity of the person requesting the information?	
Is there an agreement already in place which will meet the need? If yes, use the current ISA	
Record what information is being asked for. Is it the minimum required for the purpose? What purpose will it be used for? Is it a policing purpose?	
What is the legal basis or policing purpose to support the sharing of information.	
Has written consent of the individual(s), to whom the disclosure relates, been provided? If not, record reason why not? If victim/witness information requested, have they been given the opportunity to consent/refuse? If not, record why not? Is there a pressing need for the victim/witness information as well; is it relevant? If so record.	
Is the enquirer requesting personal information? Would de-personalised information suffice?	
Is the information requested proportional and relevant to the purpose for which it is required?	
Is there an equally effective but less intrusive alternative method of achieving the aim? If so what?	
Can the objective(s) of the information sharing be achieved without identifying the individual(s) concerned?	
Is there time to put the request in writing? Fax it, for example? If not why not?	
When do they want the information and how do they want it communicated? Is it a secure method? If not, do the risks of not disclosing outweigh the risks of insecure communication? Document these.	
What is the vulnerability and likely impact on the subject of the disclosure? What is the likely impact of not disclosing? Does the risk of disclosing outweigh the risk of not disclosing? Document this.	
Record the decision to disclose or not to disclose.	
Record what information was shared (or not shared) - attach to this completed template if more space is required.	
Is this likely to be a regular request? If so an agreement must be drafted and agreed for future use.	
Name of person making disclosure with details of any authorising person.	

Date:	