Community Safety Information Sharing Protocol PREVENT

1. Introduction

This document has been prepared to facilitate information sharing between partner agencies where there are concerns that an individual is at risk of being radicalised or being drawn into violent extremism.
This protocol mirrors similar agreements already in place to protect the vulnerable (i.e. M.A.P.P.A and M.A.R.A.C)

2. Information Sharing: the Basics

Key points for consideration when deciding to share information:

- Who is asking for the information?
  - Is the agency signed up to the ISP?
  - Are they a statutory or voluntary partner?
- What information is being asked for?
- Is the information being requested personal or sensitive, personal information? (see appendix A)
- Can information be shared securely? (pnn, gsi, gsx secure e mail)
- Have I kept a record of the decision to share information, how I reached the decision and what information was shared?

3. Why can I feel confident about sharing information?

- Agencies have signed the ISP
- Agencies are aware of their responsibilities as signatories to the ISP including the importance of ensuring that any information shared is kept securely
- Agencies have appointed Designated Officers empowered to share information
- Section 115 of the Crime and Disorder Act 1998 and the Data Protection Act 1998 (exemptions 29 and 35) both contain specific reference to personal information sharing on a case by case basis for the purposes of crime and disorder.
- Section 38 of the Counter Terrorism and Security Act 2015 places a responsibility on agencies to work together to prevent persons from being drawn into terrorism.

3. Types of information to be shared

For a list of the types of information that is likely to be shared for particular purposes see, Appendix B and C.

4. Key Legislation

- Crime and Disorder Act 1998
- Police and Justice Act 2006
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Counter Terrorism and Security Act 2015

4.2 Legislation governing the sharing of information

4.1 Sharing Information

4.1.1 Crime and Disorder Act (1998)

Section 115 of the Crime and Disorder Act 1998 provides a legal basis (not a statutory duty) for information sharing with relevant authorities where it is necessary for fulfilling duties contained in the Act. There is a wide range of activities in which the sharing of personal information is not only useful but legally permissible, particularly where decisions regarding particular interventions with individuals are being discussed. This power however does not over ride other legal obligations such as compliance with the Data Protection Act (1998), the Human Rights Act (1998) or the common law duty of confidentiality. Section 17 of the Crime and Disorder Act 1998 also imposes a duty on responsible authorities to have due regard to the effect their work may have on crime and disorder, anti-social behaviour and substance misuse.

4.1.2 Criminal Justice and Court Services Act (2000)

This Act provides for a specific duty for the Police and Probation Services to make joint arrangements for the assessment and management of the risks posed by sexual, violent and other offenders who may cause serious harm to the public.

4.1.3 Police and Justice Act (2006)

This Act introduces a duty to share depersonalised information which is intended to increase the effectiveness of partnerships by ensuring that they have the necessary multi-agency information for identifying priorities, mapping trends and patterns in crime and disorder, and managing their performance. This duty only applies when the authority holds the information so it does not require the collection of any additional information. In each case, the duty applies to information relating to the partnership area as defined by the district or unitary authority area. The specified information sets are listed in Appendix 1.

The Police and Justice Act 2006 also places a statutory duty on the strategy group of all crime and disorder reduction partnerships to prepare an information sharing protocol[1]. The protocol must cover the sharing of information under the new duty to share specified depersonalised datasets and also any additional information sharing between the responsible authorities and other agencies named under Section 115 of the Crime and Disorder Act 1998, including personal information. A statutory duty has also been placed on each responsible authority to nominate a designated liaison officer whose role is to facilitate the sharing of information with other partners.

4.1.4 Other relevant Acts

Whilst the legislation highlighted in sections 4.1.1 to 4.1.3 above are the principle ones covering the exchange of information in respect of crime and disorder, there are a considerable number of other Acts that require or enable the sharing of information, including:

- Children Act 1989
- Children Act 2004
- Domestic Violence Crime and Victims Act 2004
- Anti-Social Behaviour Act 2003
- Sexual Offences Act 2003
- Local Authority and Social Services Act 1970 (amended 2003)
- Housing Act 1996

4.2.1 Data Protection Act (1998)

[1] Statutory Instrument 2007/1830 part 4 (1) and (2) require the drafting of an Information Sharing Protocol

The Data Protection Act (DPA) sets out principles which govern the way information is processed and should not be seen as prohibitive of the relevant sharing of personal information. The processing of information covers every way in which we handle it"

The fundamental principle behind the DPA is that personal information can only be disclosed in appropriate circumstances. The DPA contains a number of exemptions which enable the sharing of information for the purposes of Prevention and Detection of crime and the apprehension and prosecution of offenders (Section 29 and 35). The DPA also requires that information must be accurate, relevant, kept up to date, held no longer than necessary, and be kept and exchanged securely. The DPA also gives individuals or 'data subjects' certain rights with regard to their personal information.

An organisation which processes information relating to identifiable living persons is legally obliged under the Data Protection Act to register as a Data Controller with the Office of the Information Commissioner, the government office responsible for the operation and enforcement of the Data Protection Act and the Freedom of Information Act. **Each agency must ensure that they hold a current registration with the Information Commissioner[2] to share appropriate information under this protocol.**

Schedule 1 of the Data Protection Act includes eight principles in respect of the sharing of personal information:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
    a) at least one of the conditions in Schedule 2 is met, and
    b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met[3].
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4.2.2 Human Rights Act (1998)

[2] An independent official appointed by the Crown to oversee the Data Protection and Freedom of Information Acts – see their website at www.informationcommissioner.gov.uk

[3] Even in the event that the Section 29 (prevention and detection of crime) Data Protection Act exemption is relied upon, Schedules 2 and 3 conditions must still be satisfied.

This Act should be taken into account in establishing whether the purpose of information exchange is lawful.
The Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be compatible with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may be subject to a legal action under section 7 of the Act. This obligation should not be seen solely in terms of an obligation not to violate Convention Rights but also as a positive obligation to uphold these rights. Article 8 of the Act is of particular relevance to information sharing as this relates to 'the right to respect for private and family life'.

4.2.3 Counter Terrorism and Security Act 2015

This Act states there is a duty for all Agency members to co-operate with the panel (Channel Panel) so far as is appropriate and reasonably practicable so the panel and the Police can carry out their functions. The duty of a partner of a panel to act in co-operation with the panel includes the giving of information and extends only so far as the co-operation is compatible with the exercise of the partner's functions under any other enactment or rule of law. Nothing in this section requires or authorises the making of a disclosure that would contravene the Data Protection Act 1998 or a disclosure of sensitive information.
Sensitive information means:

(a) held by an intelligence service,
(b) obtained (directly or indirectly)from, or held on behalf of an intelligence agency,
(c) derived in whole or part from information obtained (directly or indirectly) from, or held on behalf of an intelligence service or
(d) relating to an intelligence service.

4.2.4 Common law duty of confidentiality

The duty of confidentiality has been defined by a series of legal judgements and is a common law concept rather than a statutory requirement. Personal information which is seen as subject to this duty includes:

a) information that is not already in the public domain,
b) information that has a certain degree of sensitivity,
c) Information that was provided on the expectation that it would only be used or disclosed for particular purposes (this applies to both the living and the dead).

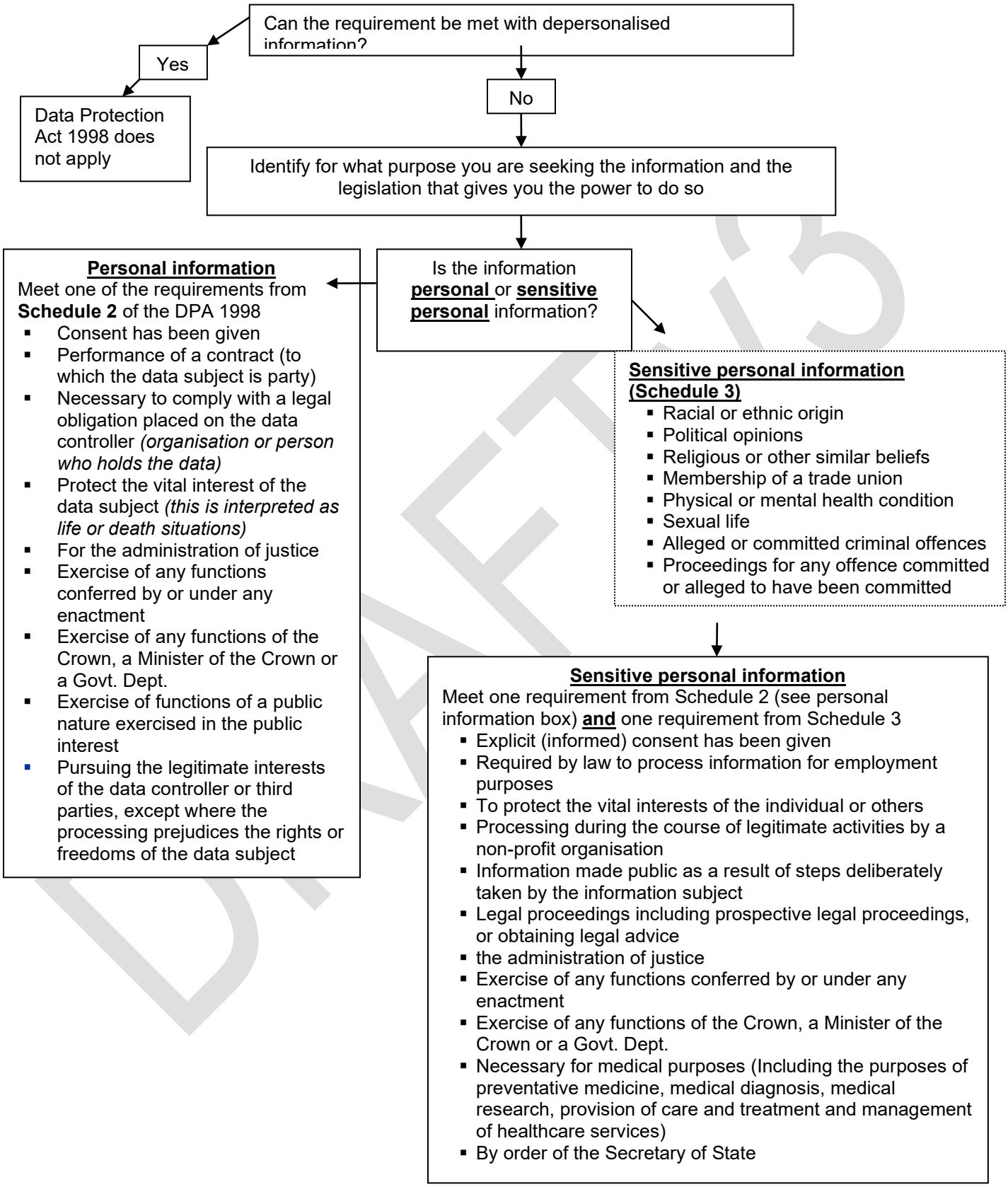
Common Law judgements have identified a number of exceptions:

a) Where there is a legal compulsion to disclose
b) Where there is an overriding duty to the public, this includes the need to prevent, detect and prosecute serious crime.
c) Where the person to whom the information refers has consented.

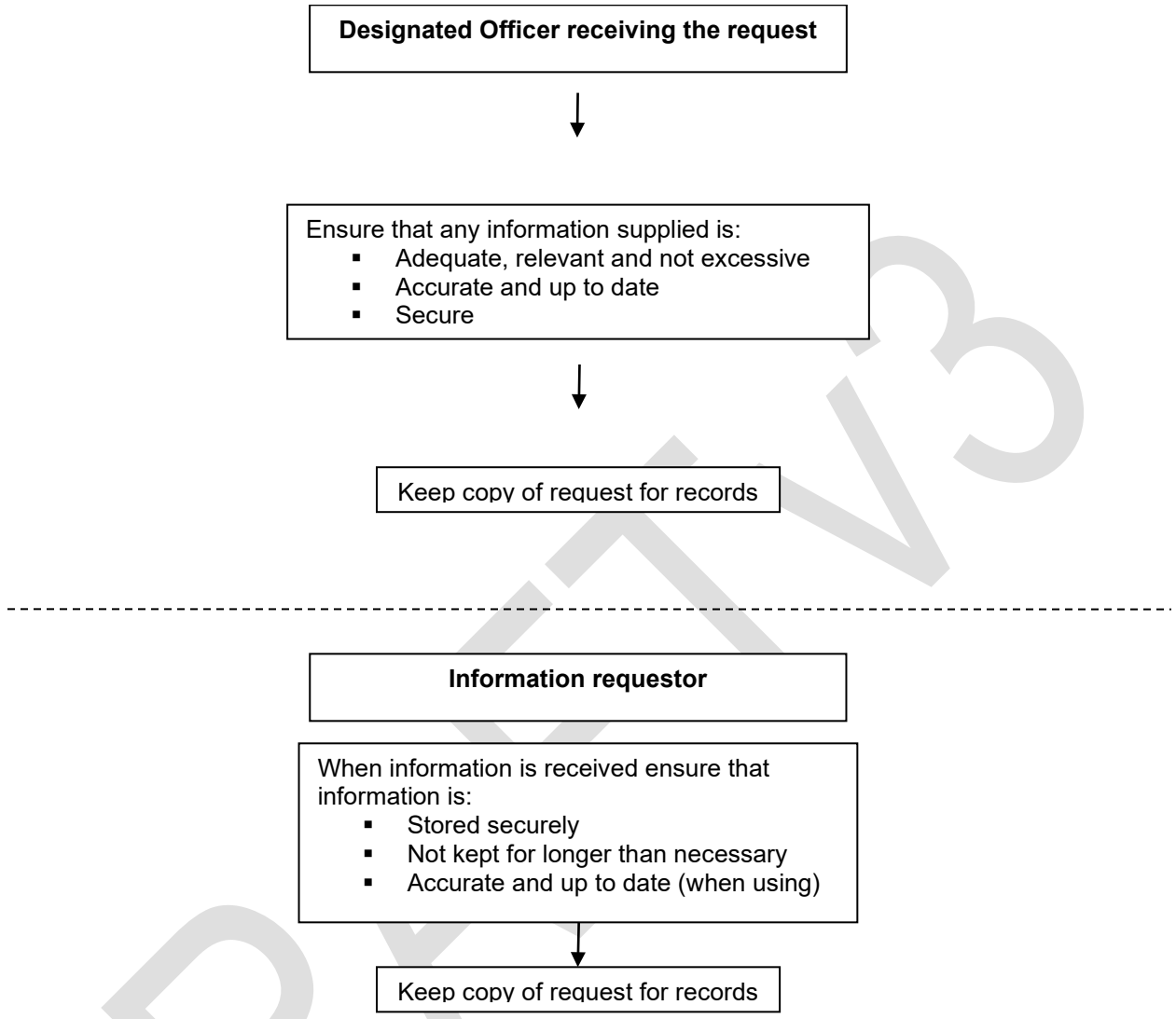
Where information is held in confidence e.g. as is the case with personal information provided to the National Health Service and medical practitioners by patients, the consent of the individual concerned should normally be sought prior to information being disclosed. Where consent is withheld or is unobtainable, designated officers should assess on a case-by-case basis, whether disclosure is necessary to support action under the Crime and Disorder Act or Counter Terrorism and Security Act and whether the public interest arguments for disclosure are of sufficient weight to over-ride the duty of confidence.

This Information sharing protocol has been agreed by representatives of all partners at the multi-agency Cleveland Contest Group.

INFORMATION SHARING PROCESS FLOWCHART



INFORMATION SHARING PROCESS FLOWCHART



Appendix A: Types of Information

Personal information

The Information Commissioner's Office (ICO) has published new guidance "*Data Protection Technical Guidance: Determining what is personal data"* that explains its view of what counts as personal data under the Data Protection Act (DPA). Everyone who is responsible for sharing personal data must be familiar with these guidelines and their operation.

The DPA defines personal data as "data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual". It is the interpretation of that definition that is the subject of the ICO guidance. Knowing what is and what is not personal data is vital because the DPA's rules apply only to the processing of personal data.

The ICO says in its new guidance that many kinds of information can count as personal data, even in situations in which people may not consider it to be so. It said, for example, that information could count as personal data even if it does not include a person's name. The ICO said that it was important to bear in mind that a person trying to identify another person might work quite hard to identify that person. Definitions of personal data, then, must be allowed to be quite wide in some cases. It also said that parts of documents can count as personal data without the whole document counting as such

The Office also said that a decision must be revised on occasion, and it must not be assumed that any decision on personal data is final. "Means of identifying individuals that are feasible and cost-effective, and are therefore likely to be used, will change over time. If you decide that the data you hold does not allow the identification of individuals, you should review that decision regularly in light of new technology or security developments or changes to the public availability of certain records."

The situation is complicated further by the fact that some information can count as personal data in one person's hands, but not in another's. The guidance gives the example of two near-identical photographs of a street party, one taken by a policeman, the other by a journalist. "The data in the electronic image taken by the journalist is unlikely to contain personal data about individuals in the crowd as it is not being processed to learn anything about an identifiable individual," it said. "However, the photo taken by the police officer may well contain personal data about individuals as the photo is taken for the purpose of recording the actions of individuals who the police would seek to identify, if there is any trouble, so they can take action against them."

Depersonalised (non-personal or anonymous) information

This is any information, which does not (or cannot be used to) reveal the identity of a living individual. There are no legal restrictions on sharing depersonalised information (See Guidance note on relevant case law on, page 70).

Depersonalised information held by public-sector agencies is covered by the Freedom of Information Act 2000, and it may need to be shared if a lawful request is made (See pages 61-63 for more information).

If the purpose of the Crime and Disorder Act can be achieved using depersonalised information then this must be the preferred method. Depersonalised information is an essential source of information for

identifying crime hotspots. The information can be utilised in Geographic Information Systems (GIS) for highlighting specific problem areas. Depersonalised information may need to be shared if it could be used to:

a) help strategic planning;
b) identify areas of high crime or disorder;
c) produce the Strategic Assessment
d) measure the effect of closed-circuit television or other schemes to prevent crime; and
e) assess whether the local crime reduction strategy is delivering effectively and efficiently.

The following guidance must be followed in relation to depersonalised information:

a) Any agency or individual handling depersonalised information may not use that information to try to identify any individual;
b) Information must not be released to those who have a commercial interest in its use;
c) Arrangements must be made for the secure storage of all depersonalised information;
d) Information must be destroyed when it is no longer required or in line with agencies' policies for managing records.

Sensitive personal information

Sensitive personal information is defined in the Data Protection Act as information that describes:

a) racial or ethnic origin
b) political opinions
c) religious beliefs or other beliefs of a similar nature,
d) membership of a trade union
e) physical or mental health or condition,
f) sexual life,
g) commission or alleged commission of any offence
h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Sensitive personal information (for the specific purposes of this protocol)

a) information relating to victims
b) information relating to witnesses
c) information held by an intelligence service, obtained (directly or indirectly) from, or held on behalf of, an intelligence service. Derived in whole or part from information obtained (directly or indirectly) from, or held on behalf of an intelligence service or relating to an intelligence service.

Under the Data Protection Act, other conditions apply to the processing and sharing of sensitive personal information. Details that are relevant in line with the Crime and Disorder Act 1998 can be released to another designated officer, however, this information must be treated carefully, and a Designated Officer must make sure that the information is accurate and relevant to an enquiry before it is released.

Other sensitive information

Some information both personal and depersonalised may still carry a degree of sensitivity although it is not specifically listed as a category of sensitive personal information under the DPA 1998. This might relate to the complexity of the data and the associated difficulties in interpretation or the need for an informed commentary or 'health warnings' to avoid misinterpretation. For the most part this can be flagged in any associated meta-data (see below), but the ISP recommends that, in the case of a request under the Freedom of Information Act in particular, these issues are considered (especially if the data originated from another source) before information is released. This is particularly important when depersonalised information may be able to be used with other information in the public domain to identify individuals.

Information which is available to the public

This type of information incorporates any information which is publicly available, whether it relates to an individual or not. Examples include:

a) the internet;
b) newspapers;
c) television;
d) Teledex;
e) government guidance, statistics, reports, White Papers and so on
f) agencies' Freedom of Information Act publication schemes; and
g) information from public records.

You should always consider whether there are any copyright, contractual or other legal conditions restricting its use. You must check that this information is up to date.

Metadata (information about data)

Metadata is information that describes a data set. A metadata specification makes the process of identifying information easier as it provides a structure of defined elements that describe or provide an explanation of the information source. It can also be used to advise the user of the data about issues of definition and interpretation, or restrictions on dissemination.

Appendix B: Example Counter Terrorism and Security Act 2015 Schedule for information sharing.

This schedule has been provided to detail the information shared for preventing people from being drawn into Terrorism.

Date of Agreement: dd/mm/yy

Partners
Police
Probation
Youth Offending Service
Prison Service
Criminal Justice Intervention Team
Courts
Treatment agencies
Housing providers
Local Education, Training and Employment Providers
Any other agency

Purpose
This agreement has been formulated to facilitate the exchange of information between partners to support multi agency intervention in respect of Prevent and Channel processes. This includes:

- To collate and disseminate relevant information on all subjects who come to notice of the partner agencies
- To analyse information and assist with the assessment of an individual's vulnerabilities and/or behaviour,
- To contribute to the welfare and appropriate package of care bespoke to each individual.
- To enable individuals to obtain information about and make use of the services and facilities available.

Agencies are entitled to request information from each other for crime prevention/detection purposes, for the administration of justice and/or for reasons of care co-ordination and assessment of risk.

Type and extent of information to be shared

A request for consent to share information may be made directly to the client; however consent is not necessary to lawfully share information for the purposes of crime and disorder, anti-social behaviour and substance misuse.

Any information shared must be justified on the merits of each case, considering necessity and proportionality.

Information exchange is of personal/sensitive personal data and is likely to include:

- Individual's name, address, date of birth
- Children's/dependent's details
- Details of convictions, cautions and formal warnings
- Details of relevant intelligence, providing the dissemination coding allows the release of information
- Whether the offender is engaging in a treatment / care plan
- Drugs being used by the offender
- Level of drug use including drug test data
- Information relating to attendance at appointments
- Information about the needs of the offender including housing, education, training and employment etc.
- Details of changes in domestic circumstances or crisis points

Use of information
Personal information must only be disclosed to another partner agency where the reason for disclosure complies with the purposes outlined in the 'Purpose' section of this Appendix. Wherever possible, the partner agency should obtain the offender's consent to their information being disclosed to other agencies.

Personal information that has been provided by one partner agency to another may only be transferred with the express agreement of the originating agency. This is irrespective of whether that material is in the format originally provided by the agency, or has been incorporated into a document created by one or more of the partner agencies.

Data retention, review and disposal
Partners to this agreement undertake that personal data shared will only be used for the specific purpose for which it is requested. Information must be stored securely and deleted when it is no longer required for the purpose for which it is provided.

Access and security
Information should be only be shared and stored in line with the principles set out in the North East ISP Guidance Notes. All documents should indicate the level of protective marking for ease of handling between agencies.

Schedule Owner: indicate who is responsible for maintaining the schedule

Date for review of schedule: dd/mm/yy

Appendix C: Example Multi-Agency BRONZE Meeting (Channel Panels) Information Sharing Schedule

This schedule has been provided to detail the information shared for Multi-Agency BRONZE meetings (Channel panel).

Date of Agreement: did/mm/my

Partners (names to be provided in full for 'real' schedules)
Police
Children's social care
Specialist domestic violence services (all agencies to be named in full)
Health
Housing
Probation
Education
Mental health
Homelessness team
Local drug and alcohol services
Clinical Commissioning Group
Children and family court advisory and support service (CAFCASS)

Purpose
This agreement has been formulated to facilitate the exchange of information between partners to support multi agency Bronze Meetings. This includes:

- To share information to increase the safety, health and wellbeing of individuals;
- To determine whether the subject poses a significant risk to any particular individual or to the general community;
- To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;

Agencies are entitled to request information from each other for crime prevention/detection purposes and for reasons of care co-ordination and assessment of risk.

Type and extent of information to be shared

A request for consent to share information may be made directly to the client; however consent is not necessary to lawfully share information for the purposes of crime and disorder, anti-social behaviour and substance misuse.

Any information shared must be justified on the merits of each case, considering necessity and proportionality.

Information exchange is of personal/sensitive personal data and is likely to include:

- Client's name, address, date of birth

- Perpetrator's name, address, date of birth
- Children's/dependent's details
- Detail of incidents of domestic abuse
- Relevant details of client's medical history e.g. injuries resulting from incidents of domestic abuse, pregnancy
- Details of client's substance misuse
- Details of perpetrator's violent offences
- Details of perpetrator's substance misuse
- Information about the needs of the client including housing, education, training and employment etc.

Use of information
Personal information must only be disclosed to another partner agency where the reason for disclosure complies with the purposes outlined in the 'Purpose' section of this Appendix. Wherever possible, the partner agency should obtain the client's consent to their information being disclosed to other agencies.

Personal information that has been provided by one partner agency to another may only be transferred with the express agreement of the originating agency. This is irrespective of whether that material is in the format originally provided by the agency, or has been incorporated into a document created by one or more of the partner agencies.

Data retention, review and disposal
Partners to this agreement undertake that personal data shared will only be used for the specific purpose for which it is requested. Information must be stored securely and deleted when it is no longer required for the purpose for which it is provided.

Access and security
Information should be only be shared and stored in line with the principles set out in the North East ISP Guidance Notes. All documents should indicate the level of protective marking for ease of handling between agencies.

Schedule Owner: indicate who is responsible for maintaining the schedule

Date for review of schedule: dd/mm/yy