NATIONAL SUPPORT FRAMEWORK
DELIVERING SAFER AND CONFIDENT COMMUNITIES

Home Office

Information sharing for community safety
Guidance and practice advice

NATIONAL SUPPORT FRAMEWORK
DELIVERING SAFER AND
CONFIDENT COMMUNITIES

Information sharing for community safety
Guidance and practice advice

ACKNOWLEDGMENTS

This guidance has been prepared by Spencer Chainey of the Jill Dando Institute for Crime Science, University College London.

Special thanks are due to Paul Hart, from Knowsley Metropolitan Borough Council, and Beth Carlisle, from the City and County of Swansea, for reading the text and commenting from the perspective of practising analysts.

Kirsty Gillan from the Regional Research and Analysis Programme provided helpful comments throughout the process of drafting, and colleagues from the following organisations and Home Office units provided valuable input:

Anti-social Behaviour Unit
Crime Strategy Unit
Joint Public Protection Information Unit
Legal Adviser's Branch
Ministry of Justice
National Policing Improvement Agency
Neighbourhood Crime and Justice Group
Offender-based Interventions Unit
Office for Security and Counter Terrorism
Prevent Interventions Unit
Public Confidence Unit
Violent Crime Unit
Welsh Assembly Government

Contents

1. Introduction

Intelligence-led and outcome-oriented practice lies at the heart of Community Safety Partnerships (CSPs) being the most effective possible vehicle for tackling crime and re-offending at the local level in England and Wales. To achieve this, efficient and effective information sharing between relevant partners is essential.

Information sharing involves the transfer of information from one agency to another. This can be information that is transferred via electronic means, in paper records, or verbally between CSP partner agencies. This can include the sharing of both personalised and depersonalised information as well as non-personal information.

Information sharing in many CSPs in England and Wales has made significant strides since the 1998 Crime and Disorder Act. Some guidance has helped CSPs along the way, but many CSPs continue to struggle and come up against barriers that constrain them in making better use of the rich sources of information that can be shared between partner agencies.

This guidance, aimed at community safety practitioners and their managers, is designed to be comprehensive in helping CSPs improve their information sharing so that they can use data in order to be confident and well informed in the decisions that they make to improve community safety at the local level. The guidance identifies what data should be shared, provides clarity on legislation, and offers advice on the processes that can be put in place to help facilitate information sharing. The guidance addresses information sharing between local CSP partners, rather than between central government and regional government agencies.

The guide draws from practice and experience across England and Wales. Importantly, the guide gets into the detail of information sharing by:

- identifying the data (right down to the data fields) that partner agencies and local neighbourhood practitioners should share;
- describing the key principles to follow when sharing information;
- providing clarity on legislation so that practitioners can be confident in what can and what cannot be shared;
- explaining the processes to apply in order for data to be fit for purpose for local-level intelligence-led service delivery; and
- suggesting a framework that can be used to help improve upon existing arrangements for information sharing.

The appendix describes the technical process of depersonalising geographic data, and explains the roles that analysts and non-analysts should play in a CSP to help facilitate information sharing and the associated development of intelligence products. The appendix also contains a glossary of words and terms used in this guidance and practice advice, and a list of abbreviations useful for community safety practitioners.

1.1 BENEFITS OF INFORMATION SHARING

"Information sharing is the cornerstone of delivering shared understanding of the issues and arriving at shared solutions … The right information enables partners to carry out evidence-based, targeted community safety interventions and to evaluate their impact. The improved outcome of an intelligence-led, problem-solving approach to community safety can only be achieved when partners have access to relevant, robust and up-to-date information from a broad range of sources". *Delivering Safer Communities: a guide to effective partnership working*. Home Office, 2007.

Effective information sharing is fundamental to supporting the development of CSP intelligence and providing an evidence base on which these partnerships can make decisions. This decision making should then help direct appropriate responses to prevent and reduce crime, disorder and anti-social behaviour (ASB); apprehend and prosecute offenders; reduce re-offending; address issues associated with the misuse of drugs and alcohol; and enhance public reassurance and confidence in the services that are in place to improve community safety.

To tackle these issues associated with community safety requires a response that involves more than one agency. Each of these agencies collects information that relates to certain community safety problems, so in order for these problems to be understood it requires each agency to share this information. If a certain problem is only considered from the view of a single agency then key aspects of the problem can be missed, the problem can be poorly understood or even misunderstood, resulting in decisions being made on little substance, and ineffective responses being deployed.

Information sharing therefore supports three important aspects of CSP working:

- **Understanding the problem** – tackling the issues associated with crime, disorder, ASB, the misuse of drugs and alcohol, reducing re-offending and public reassurance requires the nature of each problem to be well understood. To understand the problem requires information to be brought together from a range of agencies. This entails exploring patterns relating to the problem, and then deciding on tactical, investigative or strategic responses (for example, to inform Integrated Offender Management arrangements – IOM), actions for managing the most harmful and problematic individuals (for example, Prolific and other Priority Offenders – PPOs), and for supporting those that are most vulnerable to victimisation.
- **Multi-agency in content, multi-agency in outlook** – considering the problem using information from a range of agencies rather from just one agency leads more naturally to a multi-agency response. If the problem is only considered from the view of a single agency then the natural reaction is often for that agency to be considered as the only one that is in a position to tackle the problem. The inclusion of information from a range of agencies helps them to identify the role that they can play in responding to the problem and delivering a more joined-up approach to addressing it.
- **Supports partnership working** – if the problem is considered using a range of agency information then this tends to overcome the reliance on one agency as the single source of information and sole purveyor of a solution to the problem. Relying on just one agency to provide information and respond to the problem with little input from other agencies can undermine the CSP and the spirit of partnership working. Information sharing helps to foster and improve inter-agency relationships.

Benefits of information sharing – a practical example

Consider the example of developing a multi-agency response to reduce the re-offending of Prolific and other Priority Offenders (PPOs). A number of agencies collect information relating to these individuals: the police collect information on the offences that PPOs are known to have committed, Probation may have carried out a recent OASys assessment on each PPO, and the Drug and Alcohol Action Team may have the PPOs registered with them and hold data relating to their drug misuse. To understand the issues associated with prolific offenders requires these data to be drawn together. They can be used to help identify issues that relate to individuals as well as highlighting patterns that can be seen across all PPOs. These could be issues associated with drug misuse, unsuitable housing, and lack of employment skills that are common to many prolific offenders, and the partnership will need to decide upon the most appropriate multi-agency response. If issues associated with prolific offenders were only considered by using data from one agency then certain aspects of the problem could be missed, which in turn could impact upon key decisions about the suitability and timeliness of interventions to address an individual's offending behaviour.

Ultimately, the personal safety of millions of people rests on the decisions taken by statutory agencies on the ground. All partners engaged in work related to community safety and wellbeing have a responsibility to share information where they think that action may need to be taken – if a housing officer, for example, notices something untoward on a visit, suitable and clear processes should be in place to ensure that, where appropriate, the information is shared with the relevant partner agency. Failure to do so may compromise both the safety of the individual and the professional reputation of the agencies in the partnership.

1.2 CONTENT OF THE GUIDE

There are four main sections to this guide. Section 2 provides important definitions that relate to information sharing and why information should be shared. Section 3 describes what information should be shared, and Section 4 describes how it should be shared.

2. Definitions, purposes of and the legal basis for information sharing

In this section we define the types of information to be shared, the agencies that are involved in CSP information sharing, and the legal basis for information sharing.

2.1 TYPES OF INFORMATION FOR SHARING

In general there are three main categories of information that are relevant to CSPs:

- **Aggregate information that is publicly available** – this is information that has been aggregated into certain groups such as gender, age, or to a geographic area such as a local authority ward, and is published in the public domain. This includes administrative data and Census of Population data published by the Office for National Statistics on the Neighbourhood Statistics Service, and other more particular services such as Public Health Observatories. This type of information can be freely shared as it is already in the public domain.
- **Aggregate information that requires authorisation to access** – this is information that is aggregated into certain groups such as gender, age, or to a geographic area such as a local authority ward, but which can only be accessed by CSPs using the authorisation procedures that are relevant to that data source. For example, this includes data published on iQuanta and DIRWeb, where a username and password are required, and only given to those who are authorised to access this information. This type of information can only be shared among the agencies that are identified in the CSP, and should not be shared with agencies that are not authorised to have access to these data.
- **Case level information recorded by local agencies** – this type of information can be categorised as falling into three types – personal information, sensitive personal information and depersonalised information. These types of information can either be recorded as data records stored electronically on a database such as JTrack, or as information recorded on a form or a report in either paper (or some other hard copy) or electronic format. For example, this type of information may include police recorded crime data, case and offender management records, details about a domestic violence incident, Probation data, data recorded by a local authority about anti-social behaviour incidents, and Fire and Rescue Service incidents. This type of information can only be shared among the agencies that are identified in the CSP.

Definitions of types of information recorded by local agencies

A. Personal data (defined by the Data Protection Act 1998)

Personal data is any information that either by itself or in combination with other information held or likely to come into the possession of the holder, however recorded, can identify a living individual. The sharing of personal information within a CSP is possible when decisions regarding particular interventions with individuals are discussed or made.

Definitions of types of information recorded by local agencies *(continued)*

B. Sensitive personal data (defined by the Data Protection Act 1998)

Sensitive personal data is a subset of personal data. It is defined as information describing, in relation to the data subject:

- racial and ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health condition;
- sexual life;
- commission or alleged commission of any offence; or
- any proceeding for any offence committed or alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings

In relation to community safety, information that should also be treated as sensitive personal data includes:

- Information relating to victims
- Information relating to witnesses

C. Depersonalised data (defined by the Crime and Disorder (Overview and Scrutiny) Regulations 2009)

Depersonalised information refers to information that does not constitute personal data under the Data Protection Act 1998. Depersonalised information can not be used in any way to identify a living individual. No recipient of the depersonalised information should have the ability to 'recreate' certain attributes of the personal data using other information they may be able to access, and hence identify an individual. Depersonalised information is created by 'anonymising' (sometimes also referred to as 'sanitising') personal data. Depersonalised information could include aggregated counts of the number of crimes in a specific area such as a local authority ward, or the original recorded data, albeit stripped of attributes that identify an individual.

D. Protectively marked information

Protectively marked information – normally marked as 'RESTRICTED' or 'PROTECT' – in a CSP must be shared and stored in accordance with government procedures. In a CSP, intelligence documents should usually be marked as 'RESTRICTED' because they contain information that should only be made available to its intended audience, and can only be more widely published with the permission of the supplier from which the information originated.

The Protective Marking System (often referred to as the Government Protective Marking System/Scheme or GPMS) is the Government's administrative system to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction (see p.54).

2.2 AGENCIES INVOLVED IN INFORMATION SHARING FOR COMMUNITY SAFETY

We explain key features of the legislation relevant to agencies involved in community safety information sharing in Section 2.4, but in this section we begin by defining these groups and identify the agencies to whom information sharing for community safety is applicable. The agencies who may share information relating to community safety should be specified in an Information Sharing Protocol, which each agency wishing to share information should be signed up to.

Information sharing protocols

An information sharing protocol (ISP) should provide an agreed framework which underpins the work of CSPs and their partner agencies in the exchange and use of information. In particular, the ISP should:

- facilitate the secure sharing of information between CSPs and partner agencies;
- govern the secure use and management of information by CSPs;
- enable the responsible authorities in a CSP to meet their legislative obligations effectively, e.g. Section 17 of the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009); and
- ensure that clear processes are in place for the partnership to respond to Freedom of Information requests, including those occasions when a request is made for information from one agency which originated from another partner agency (in this situation the agency who received the request should consult with the originating authority before any information is released).

This guidance does not provide a template for information sharing protocols. Instead, readers are referred to the Home Office Crime Reduction website where examples are available: www.crimereduction.gov.uk. (The North East Community Safety Partnership Information Sharing Protocol provides a comprehensive example and will be available on the website from May 2010.)

2.2.1 Responsible authorities

Responsible authorities are under a statutory duty to ensure that they come together and work in partnership in a CSP. To work in partnership requires information to be shared between these agencies. The responsible authorities are:

- District council, borough council, unitary authority or county council
- Police force
- Police Authority
- Fire and Rescue Authority
- Primary Care Trusts in England and Local Health Boards in Wales
- Probation Trusts.

Designated Liaison Officers for information sharing – each responsible authority has the statutory duty to nominate a Designated Liaison Officer, whose role is to proactively facilitate information sharing between partner agencies, ensure legislation is adhered to and that at least the minimum information sharing requirements are complied with.

2.2.2 Co-operating bodies

Co-operating bodies are those agencies that are important in supporting the business processes of the CSP, including the development of intelligence about community safety issues and the implementation of the Partnership Plan. To support the business processes of the CSP information needs to be shared between these agencies. The co-operating bodies, prescribed by order, are:

- parish councils
- NHS Trusts
- NHS Foundation Trusts
- Registered Social Landlords
- proprietors of independent schools
- governing bodies of schools and further education institutions
- agencies appropriate for the particular location or circumstances of the CSP, for example, the Forestry Commission

Responsible authorities should also invite the co-operation of relevant voluntary, community and private groups, but whose access to information may need to be limited. These limitations should at the very least be defined in an ISP.

2.2.3 Relevant authorities

The effect of Section 115 of the Crime and Disorder Act 1998 is to allow information to be shared for the purposes of community safety between a number of 'relevant authorities'. We explain the Crime and Disorder Act and its relevance to information sharing in more detail in section 2.4. The relevant authorities are defined as:

- Police forces
- Police authorities
- Local authorities – district councils, borough councils, unitary authorities and county councils
- Probation Boards and Trusts
- Fire and Rescue authorities (in practice it is the local Fire and Rescue Service itself that sits on the partnership)
- Health authorities – Primary Care Trusts (in England), Local Health Boards (in Wales), Strategic Health Authority, NHS Trust, and NHS Foundation Trusts
- Registered Social Landlords
- Transport for London.

2.2.4 Information sharing with agencies outside the CSP's jurisdictional area

On occasion there may be a requirement to share information with agencies operating outside the jurisdictional area of the CSP. For instance, this could include a neighbouring police force or local council. On these occasions, and in accordance with the Data Protection Act (see Section 2.4), information sharing is possible, but only within the conditions of the ISPs for each of the relevant jurisdictional areas for the CSPs that wish to share this information.

Agencies to include as signatories on the Information Sharing Protocol

The ISP should be signed by those agencies that are approved by the responsible authorities as those who should be involved in local information sharing. It is often useful to list two groups of agencies, to distinguish between those that have a central role in information sharing and those that do not. This helps to keep a tighter reign on the circulation of information, but it should not constrain partnership work, and should still allow the second group to access depersonalised information.

The agencies to include on an ISP and who should play a central role in the sharing of information for community safety are:

- Police Force
- Police Authority
- District council, borough council, unitary authority or county council
- Fire and Rescue Service/Authority
- Primary Care Trust/Local Health Board
- Probation Trust
- Strategic Health Authority
- NHS Trusts
- Mental Health Trusts
- Ambulance Service
- Youth Offending Service
- Drugs and Alcohol Action Team
- Criminal Justice Board
- Crown Prosecution Service
- HM Courts Service
- HM Prison Service and contracted prisons
- Young Offender Institutions
- Housing Associations and other Registered Social Landlords
- Victim Support
- Voluntary agencies who provide specialist services such as those for drug and alcohol treatment, and victim support for sexual assault and domestic abuse.

The second group of agencies are usually those that are only required to share information on a very occasional basis, and are most often not required to share personal information. This could include local business and community groups, and other voluntary groups who do not provide specialist services.

Any agency wishing to become a 'partner' (and hence involved in information sharing) should only do so with the consent of all the responsible authorities.

2.2.5 The Wales Accord for the Sharing of Personal Information

In Wales, the Accord on the Sharing of Personal Information (WASPI) provides an added basis to enable service-providing organisations directly concerned with the wellbeing of an individual to share information between them in a lawful and intelligent way. WASPI is a framework that facilitates this by establishing agreed requirements and mechanisms for the exchange of personal information between parties in an information sharing community. This community can consist of any number of organisations, and can include public sector, voluntary sector, private and independent organisations. There is no limitation to who is able to sign up to the WASPI and implement its requirements.

The WASPI framework is made up of two parts:

- The Accord – the common set of corporate principles and standards under which partner organisations will share information. It records the commitment of Senior Officers in each participating organisation to meet agreed standards for the sharing of personal information
- The Personal Information Sharing Protocol (PISP) – a PISP focuses on the purposes underlying the sharing of specific sets of information. It is intended for operational management and staff and provides the details of the processes for sharing information, the specific purposes served, the people it impacts upon, the relevant legislative powers, what data is to be shared, the consent processes involved, any required operational procedures and the process for review. The PISP communicates to practitioners the operational requirements, setting out the who, what, why, where, when, and how of sharing information.

Only one Accord is required for a region, while there will be many PISPs.

Although originating in Wales, the WASPI framework can easily transfer across to English information sharing communities as the principles and delivery fit with most CSP situations.

More details about WASPI can be accessed from here:
www.wales.nhs.uk/waspi

2.3 THE PURPOSE OF INFORMATION SHARING IN A CSP

The purposes of information sharing in a CSP generally fall into three main categories:

- to support performance monitoring;
- to develop intelligence in the form of intelligence products (such as strategic assessments, problem profiles and tactical assessments) and to identify new incidents and emerging problems; and
- to support the delivery of services to particular groups or individuals.

These three categories differ mainly in terms of the details contained in the information that is required, the geographical level at which information is available (e.g. district or address-based data) and the timeliness of its supply.

Understanding local neighbourhood needs is a vital part of improving community safety and building neighbourhood confidence. Sharing information helps agencies to understand local community needs, determine priorities and consider how to best allocate resources through public services.[1]

2.3.1 Information for performance monitoring

Information is used for this purpose to enable the CSP to monitor trends and its performance against its targets. This may include the monitoring of performance against Public Sector Agreement targets, National Indicators (in England) and local targets set in relation to the Partnership Plan. The type of information that most usually falls into this category is aggregate information that is in the public domain or aggregate information that can be accessed using authorisation procedures.

In some circumstances, information that is required for performance monitoring may require a specific processing task to be performed. This often requires aggregating information stored on recording systems rather than sourcing information that is normally published in aggregate form. For example, information on repeat incidents of domestic violence may require the local police force to collate individual records in order to provide this measure and share it with local partners.

2.3.2 Information to assist in the development of intelligence products and identify and respond to new incidents and emerging problems

Information used for developing intelligence products such as strategic assessments and problem profiles should include personal and depersonalised information that can be sourced from local agencies and suitable sources of aggregate information. This may include information on crime recorded by the police, incidents of ASB (recorded by the local council and others, for example, housing management organisations, victim support, police), and assessments of offenders currently under supervision (recorded by Probation or Youth Offending Service) and/or subject to offender-based intervention programmes (such as PPO and DIP), for example, to inform priorities for local Integrated Offender Management arrangements.

Similar types of information may be shared ad hoc by CSPs to help identify, discuss and decide how to respond to new incidents and emerging problems. For example, at a monthly CSP meeting, information may be presented by certain partner agencies identifying a spate of new incidents on a housing estate, and this could prompt discussion with other partners about its cause and a request for any information that others may have on this new problem.

Section 3 of this guidance goes into the detail on the types of information that should be shared for these purposes in a CSP.

2.3.3 Information to support the delivery of services to particular groups or individuals

Information should be shared in a CSP to help to identify and support vulnerable individuals, manage individuals effectively, and provide services to particular groups or persons. This may include information that is used to support a CSP's Integrated Offender Management arrangements for reducing re-offending or Multi-Agency Risk Assessment Conference (MARAC) process for helping to

[1] See the *Safe and Confident Neighbourhoods Strategy* and the Communities and Local Government report on understanding public services for more details about measuring local neighbourhood needs and allocating resources to priority neighbourhoods www.communities.gov.uk

address an issue of domestic violence; for managing PPOs, including those who are problematic drug users; or for identifying children at risk. Subsequent sections of this guidance identify the types of information that should be shared for these purposes and clarify the procedures for doing so.

2.4 LEGISLATION APPLICABLE TO INFORMATION SHARING

In this section we provide a concise description of the legislation governing data sharing to help clarify the legal basis for sharing information. You should seek further advice from your authority's Data Protection Officer if in any doubt over the legislation. In this section we do not provide all of the legislation in full, but instead provide information that clarifies the main principles that apply to information sharing for community safety. These principles apply to personalised information. The sharing of depersonalised information is not subject to the same legal restrictions, however, certain principles that are discussed in subsequent sections describe how both depersonalised and personalised information should be stored and accessed. We also refer readers to Section 2.1, which deals with 'RESTRICTED' information and the use of all information in a CSP.

2.4.1 Powers for sharing information

There are many legal powers that enable or require information to be shared. In this section we describe the three principal Acts that provide the legal power for sharing information for the purposes of community safety:

- The Crime and Disorder Act 1998
- The Police and Justice Act 2006, and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 made under the Act
- The Criminal Justice and Court Service Act 2000

2.4.1.1 The Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act provides a legal basis for sharing information between CSP partner agencies where it is necessary for fulfilling the duties contained in the Act. The key conditions to consider under Section 115 are:

- 'relevant authorities' have the power (but not a legal duty) to share information if it is necessary for the purposes of any provision under the Crime and Disorder Act. This would include where it is necessary for the formulation and implementation of the local Crime and Disorder Reduction Strategy
- This power does not override other legal conditions governing information sharing. These principally relate to the Data Protection Act 1998, the Human Rights Act 1998 and the common law of confidentiality (see Section 2.4.2.)
- Personal information can be shared without the permission of the person to whom it relates. However, the legal conditions governing the sharing of personal information must be followed.

In addition, under Section 17A of the Crime and Disorder Act, a 'relevant authority' is under a duty to share with all other relevant authorities information of a 'prescribed description' which is relevant to the reduction of crime and disorder, including anti-social behaviour, in any area of England and Wales. Information is of a prescribed description if it is:

- depersonalised information, and
- of a type listed in the Schedule to the 2007 Regulations.

The Schedule should be consulted for more detail, but in summary, prescribed information will be information relating to:

- police recorded crime and police recorded incidents;
- Fire and Rescue Service recorded incidents of deliberate fires, assaults and malicious calls;
- local authority recorded incidents of ASB, environmental crime, racial incidents, school exclusions and road traffic collisions;
- National Health Service/Primary Care Trust records on hospital admissions relating to assaults, drugs and alcohol related harm, domestic abuse, and mental and behavioural disorders due to drug use; and
- Ambulance Service call-outs to crime, disorder and ASB incidents.

2.4.1.2 The Police and Justice Act 2006 and the Crime and Disorder (Overview and Scrutiny) Regulations 2009

The Police and Justice Act, and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 made under the Act incorporate the following duty that relates to information sharing:

- When requested by a crime and disorder committee, responsible authorities and cooperating bodies are under a duty to share with the committee information that relates to the discharge of the authority's crime and disorder functions, or that relates to the discharge by the committee of its review and scrutiny functions under section 19 of the Police and Justice Act. This duty only applies under the following conditions:
  - The information should be depersonalised information, except when the identification of an individual is necessary or appropriate in order to enable the crime and disorder committee to properly exercise its powers; and
  - It should not include information that would prejudice legal proceedings, or the current or future operations of the responsible authorities.

2.4.1.3 Criminal Justice and Court Service Act 2000

The Criminal Justice and Court Service Act provides for a specific duty for the Police and Probation to share information in order to make joint arrangements for the assessment and management of the risks posed by offenders who may cause serious harm to the public.

2.4.2 The law governing information sharing

The main legal powers that govern information sharing are contained in:

- Data Protection Act 1998
- Human Rights Act 1998
- The Caldicott Principles (where the sharing of information relates to health and social care organisations' use of patient-identifiable information)
- Common law duty of confidentiality
- Freedom of Information Act 2000

In practice, it is necessary to identify the legal basis for sharing personal information. The appropriateness of sharing can then be considered in relation to human rights, the Caldicott Principles (where appropriate), conditions of confidentiality, and freedom of information, to establish whether in each case the Data Protection Act provides the power for this information to be shared.

We describe the key and relevant features of the five principal legal powers in this section.

2.4.2.1 Human Rights Act 1998

Article 8 of the Human Rights Act is the article of particular relevance to information sharing for community safety as it relates to 'the right to respect for private and family life' for everyone. This article should be considered when sharing personal or sensitive personal data.

Article 8 states that everyone has the right to respect for their private and family life, home and correspondence, and that no public authority will interfere with this right unless it is necessary by law. This qualification will usually enable personal information to be shared on the following grounds:

- national security;
- public safety;
- economic wellbeing of the country;
- to prevent crime or disorder;
- to protect health or morals; and
- to protect the rights or freedoms of others.

2.4.2.2 The Caldicott Principles

The Caldicott Principles apply to health and social care organisations' use of personal information. These organisations are required to observe the following principles when using personal information:

- justify the purpose;
- not use personal information unless it is absolutely necessary;
- use the minimum amount of personal information that is necessary;
- access to personal information should be on a strict need-to-know basis;

- everyone should be aware of their responsibilities with regard to personal information;
- action should be taken to ensure that those handling personal information are aware of their responsibilities and obligations to respect an individual's confidentiality; and
- understand and comply with the law.

Each health and social care organisation has a Caldicott Guardian. These individuals should be consulted when there is a requirement from the agencies they represent to share personal information.

2.4.2.3 Common law duty of confidentiality

The duty of confidentiality has been defined by a series of legal judgments and is a common law concept rather than a duty contained in statute. Where information is held in confidence, such as personal information about patients held by medical practitioners, the consent of the individual concerned should normally be sought prior to any information being disclosed.

Common law judgements have, though, identified a number of exceptions and have determined that information held in confidence can in certain circumstance still be disclosed without the individual's consent. Where they can be demonstrated, factors that may justify disclosure include:

- it needs to be shared by law;
- it is needed to prevent, detect and prosecute serious crime;
- there is a public interest;
- there is a risk of death or serious harm;
- there is a public health interest;
- it is in the interests of the person's health; or
- it is in the interests of the person concerned.

Specific measures to prevent crime, reduce the fear of crime, detect crime, protect vulnerable persons, maintain public safety or prevent offenders from reoffending are in the public interest. However, there still needs to be a careful balancing exercise in each case to ensure that the disclosure (including the extent of the disclosure) is justified on the basis of an overriding interest.

The common law duty of confidentiality does not apply when this type of personal information is effectively depersonalised (e.g. records on patients that are admitted to hospital for injuries sustained from assaults, if effectively depersonalised, can be shared with partner agencies). However, in the case of personal information there is the duty to assess each request on a case-by-case basis.

2.4.2.4 Freedom of Information Act 2000

The Freedom of Information Act (FOI) permits any person to request any information held by public authorities. There are a number of circumstances when an authority may refuse to provide information because one or more of a number of exemptions may apply to the information requested. For example, the Data Protection Act (see Section 2.4.2.5) is the overriding legislation that governs access to personal information, which is generally only available to the person who is the subject of the information. This may mean that requests under the FOI result in the provision of depersonalised information, where that information is not already in the public domain.

A request from an individual or agency outside of the CSP may be made to the CSP for any information that one of the partner agencies holds. In the event that a request is made for information which originated from a partner agency, it should be a requirement for the CSP (or the partner agency receiving the request and who may have access to this information) to consult with the agency from where the information originated before any information is provided.

2.4.2.5 Data Protection Act 1998

The Data Protection Act (DPA) provides a legal framework for holding, obtaining, recording, using and sharing personal information. Under the DPA these tasks are referred to as 'processing' of personal information.

Under the DPA personal information can only be disclosed in accordance with the principles and exemptions that apply to the DPA.

DPA principles

There are eight principles that apply to the sharing of personal information:

1. It will be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 of the DPA is met and in the case of sensitive personal information, at least one of the conditions of Schedule 3 is also met.

DPA Schedule 2 conditions:

- Processing information with the permission of the data subject (the person who the information is about)
- If the processing is necessary for:
  - the performance of a contract to which the data subject is party or entering into a contract at the request of the data subject
  - meeting any legal obligation that applies to the data controller
  - protecting the vital interests of the data subject
  - necessary for the administration of justice, for the exercise of the functions of either the House of Parliament, for carrying out statutory functions and any functions of the Crown, a Minister of the Crown, or government department, or carrying out any other function that is in the public interest
  - the purposes of the legitimate interests of the data controller or anyone else who receives the information, as long as this will not affect the rights and freedoms or legitimate interests of the data subject.

DPA Schedule 3 conditions:

- Processing with the permission of the data subject
- Processing that is needed to exercise a legal right or obligation in connection with employment
- Processing that is needed to protect the vital interests of the data subject where consent cannot be given by the subject or the controller cannot reasonably be expected to gain consent
- Processing that is needed to protect the vital interests of another person where consent has been unreasonably withheld by the data subject
- Processing information in connection with its legitimate interests by any non-profit-making organisation that exists for political, philosophical, religious or trade union purposes
- Processing information that has been made public as a result of something the data subject has deliberately done.
- Processing that is needed in connection with legal proceedings, getting legal advice or exercising or defending legal rights
- Processing that is needed for the administration of justice, for the exercise of function of the Crown, Ministers or government departments
- Processing that is needed by an anti-fraud organisation which is necessary for the purpose of preventing fraud
- Processing medical information by medical professionals or others that have an obligation to keep the data subject's information confidential
- Processing of information regarding racial or ethnic origin which is necessary for the purpose of reviewing equality of treatment between persons of different ethnic or racial origin with a view to promoting such equality, provided it is carried out with appropriate safeguards for rights and freedoms of data subjects.

2. Personal information must only be processed for a specific purpose or purposes
3. Personal information must be adequate, relevant and not excessive for the purpose
4. Personal information must be accurate and, where necessary, kept up to date
5. Personal information must not be kept longer than necessary
6. Personal information must be processed in line with the rights of the person it is about. This relates to the following:

    - Personal information must be kept secure. Appropriate technical and organisational measures must be put in place to protect the information against unauthorised or illegal processing and against accidental loss, or destruction, or damage to personal information.
    - Personal information must not be transferred to countries outside the European Economic Area without suitable protection.

DPA exemptions

The DPA contains a number of exemptions which enable data to be shared for certain purposes without being subject to all the restrictions of the Act. The most pertinent exemptions that relate to community safety are:

Section 29 – Crime and taxation

- Personal data processed for any of the following purposes:
  - the prevention or detection of crime,
  - the apprehension or prosecution of offenders
- Personal data which are processed for the purpose of discharging statutory functions
- Personal data for which the data controller is a relevant authority, and which consist of a classification applied to the data subject as part of a system of risk assessment operated by that authority for preventing or detecting crime, for example, the Probation OASys Assessment.

Section 35 – Disclosures required by law or made in connection with legal proceedings

- Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court
- Personal data are exempt from the non-disclosure provisions where the disclosure is necessary:
  - for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
  - for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

We stress that this guidance provides the key and most relevant pieces of information that relate to the legislation applicable to community safety information sharing. Whilst what is included is comprehensive, and is aimed at raising general awareness, we still advise that you consult further with your Designated Liaison Officer for Information Sharing if at any point you are uncertain or have questions about the legal basis for sharing information for community safety.

The justification for sharing personal data must in all cases be evidence-based. The public must be confident that CSPs do not adopt a 'big brother' role and share data as a matter of course. Each request to share personal data must be considered individually, and if it is shared, it must be destroyed after it has been used for the purpose for which it was intended.

Any organisation which processes personal data and wishes to share these data has a statutory requirement under the DPA to ensure they have a current notification with the Information Commissioner's Office. Notification involves giving the Information Commissioner's Office details about their processing of personal information. More details about the notification process can be found at: www.ico.gov.uk/what_we_cover/data_protection/notification.aspx

Box 1. Reminding officers of their roles and responsibilities when using and handling information used for community safety

Officers from a CSP who sign the Information Sharing Protocol are not necessarily the officers who attend CSP meetings when personal information is shared. It is vital that officers who attend these meetings understand their roles and responsibilities in relation to the use and handling of personal information.

Several CSPs in England and Wales use for their business meetings an attendance and agreement form, or at least for those at which personalised information is shared. CSPs would benefit from using a form that includes a statement similar to the following (adapted from the Middlesbrough CSP Attendance and Agreement Form):

The persons listed who have attended this meeting have agreed that the overriding principle of sharing information is based on the reduction of crime, disorder and anti-social behaviour in <insert location name> and that matters discussed at this meeting will remain confidential within the organisations attending this meeting unless otherwise agreed by the meeting and recorded within an action plan. Information that is shared is done so in compliance with the <insert name of CSP> Information Sharing Protocol. Any disclosure of information outside of this meeting has to be agreed by the Designated Liaison Officer for the agency from which the information was sourced.

3. Information that should be shared

In this section we describe the information that should be shared in a CSP. We begin by outlining how to approach the sharing of information and then describe in depth the data that CSPs should share, recommending the content of datasets that should be shared.

3.1 APPLYING A PROBLEM-ORIENTED APPROACH TO INFORMATION SHARING

Evidence from practice across England and Wales suggests that a problem-oriented approach to information sharing is one that helps CSPs successfully exchange and manage information shared across the partnership. This applies to personalised, depersonalised and non-personal information. This approach helps to assess personal information sharing on a case-by-case basis, and to prioritise information by distinguishing between core and peripheral datasets required to help solve community safety problems. Not all information can be processed at the same time so prioritising is important. Peripheral data may also be important but may only be required in certain circumstances, with those circumstances being defined by the problem that needs solving.

Core and peripheral data can include personalised, depersonalised and non-personal information.

3.1.1 Core datasets

Core datasets are those that are required on a routine and regular basis to support CSP working. These data may need to be sourced to inform the operational business functions of the CSP, such as details on individuals to support the case management of offenders or for MARACs; to assess prioritisation under local Integrated Offender Management arrangements; information on emerging problems (e.g. a rise in ASB incidents in the local park); or the generation of intelligence products such as strategic assessments, problem profiles and tactical assessments:

- Information that is shared for the operational business functions of the CSP is required as and when necessary, and this may include both personal and depersonalised information.
- Information that is required for the generation of intelligence products may most typically need to be sourced on routine and regular occasions and may be appended to an existing data storage archive (containing data that had previously been supplied). This type of information may be needed to support the continual monitoring of performance, or is a key dataset that is used time and time again in intelligence products.

In this section we consider each requirement in turn in terms of the data that should be shared. We consider the practical processes involved in sharing this information in Section 4.

3.1.1.1 Information sharing to support the operational business processes of the CSP

The sharing of information to support the operational business processes of the CSP can involve the sharing of both personal and depersonalised information. Information from incident reports may be shared with partner agencies to highlight new problems that have recently emerged. For example, at a monthly partnership meeting, partner agencies may bring information to the table that highlights a number of new incidents or an emerging issue in a certain neighbourhood. If the information is not personal (e.g. describes the types of incidents and the increase) then this information is not subject to the consideration of legal conditions that relate to sharing this information. However, if the information is personal (for example, contains the names of those who are suspected to have caused the offences), then the legal basis for sharing this information must be considered.

In a CSP there are certain operational business processes that specifically require the sharing of personal information i.e. Integrated Offender Management, MARAC, MAPPA, PPO and DIP schemes, Drug and Alcohol meeting groups, and ASB panels. Each information request (for personal information), including the content of the information that is to be shared, should therefore be considered on an individual basis. It is usual, though, to share certain standard items of information for each business meeting process for which there are circumstances that require information. These are described below.

Integrated Offender Management

IOM is the strategic umbrella or overarching framework that brings together agencies across government to prioritise interventions with offenders who cause crime in their locality. It builds on, and incorporates, both the Prolific and other Priority Offender and Drug Interventions Programmes. It provides a structure for identifying agreed priorities across partnerships, including the offenders of most concern in the area. Accordingly, IOM has to be built on effective information sharing.

Multi-Agency Risk Assessment Conference (MARAC)

Personalised data to be shared should conform to the standard requirements and requests for information on the MARAC referral and research forms, and in so doing ensure that the legal basis for sharing information can be demonstrated.

Information that is most typically shared for the purposes of MARAC should include:

- name, date of birth and address of the victim, offender and children at risk; and
- personal details that relate to the abuse, including the injuries sustained, frequency of abuse, whether the victim is pregnant, and other matters of concern that each agency may have information about in relation to any of the individuals involved.

Multi-Agency Public Protection Arrangements (MAPPA)

MAPPA involves the identification of offenders that need supervision, sharing personal information between local agencies in order to support the offender's supervision and provide better public protection, assessing the risks posed by offenders, and managing the risks. Agencies involved in MAPPA are primarily the police, probation and prison services and other agencies that are under a duty to co-operate (including health agencies and local councils, particularly departments for social care, housing and education services).

There is a national standard for MAPPA which should be followed in order to ensure that the legal basis for sharing information can be demonstrated.

Prolific and other Priority Offender (PPO) Schemes

PPO schemes focus on the small hard-core group of offenders identified as committing a disproportionate amount of crime in local areas or who cause disproportionate damage to their local communities. Local PPO schemes hold strategic and operational level partnership meetings to monitor impact on individuals and community, review performance, effectively manage individuals and assess their risk as well as needs, while delivering criminal justice and social interventions which will help reduce re-offending.

Agencies that typically participate include the police, Probation, Youth Offending Service (YOS), Drug Intervention Programme (DIP), local council (e.g. community safety) housing providers, Job Centre Plus, the local Primary Care Trust (PCT), and Local Health Boards.

The sharing of personal information can occur in any of these meetings. Personal information to be shared could include:

- Name, date of birth and address of the offender
- Criminal history, including details on the last offence that the offender was convicted for and their most recent offences
- Previous terms of custody, community orders and other supervision
- Probation OASys or YOIS assessment
- Drug and alcohol use
- Drug and alcohol treatment that is being provided
- Current housing provision
- Progress on education and occupation opportunities
- Custody release date (if relevant)

Drug Interventions Programme (DIP)

DIP identifies problem drug-using offenders at the earliest stage in the criminal justice system and moves them into treatment and support and away from crime. Offenders are faced with the choice of complying with what is required of them or facing criminal sanctions.[2]

Sharing of personal information may be required to:

- Ensure effective continuity of care for an individual – information may generally only be shared with informed consent. Exceptions apply, for example, where the client may be likely to harm themselves, or another person. The client must not only be informed about and understand the uses to which the information will be put, but also the circumstances when confidentiality may be broken. They must agree to the information being shared for purposes as outlined. The worker and the individual must sign the consent form attached to the Drug Interventions Record (DIR) to confirm that this has occurred.
- Ensure an appropriate response to an individual's compliance or failure to comply with what has been legally required of them – DIP process guidance[3] includes advice on what information needs to be shared to meet the legal requirements for Testing on Arrest, required assessment and Restriction on Bail – including when consent may be required. For example specific provision has been made in instances where a positive test result is obtained and the police require initial and follow-up assessments to be undertaken, that the test result and requirement are communicated to the Criminal Justice Integrated Team, which will be carrying out those assessments. The sharing of information between the police and CJIT for this purpose does not require the consent of the individual, although good practice is to inform the client.

[2] Additional guidance may be found at http://drugs.homeoffice.gov.uk/publication-search/dip/DIP_PPO_info_share.html
[3] http://drugs.homeoffice.gov.uk/publication-search/dip/intensive-guidance-april-20092835.pdf?view=Binary

- To inform intelligence gathering – where personalised data are used for intelligence gathering the optimum position is to obtain informed consent from the offender. Where there is no informed consent, data should only be used in circumstances where there are specific public protection concerns and then only on a case-by-case basis. It would not be acceptable to actively use information such as a positive drug test in isolation to target that individual, whereas the use of personalised data might be justified where police are acting on specific information to prevent the commission of a serious offence. The key to ensuring the legality of such information sharing is that it is processed in a fair way, that is, clients should be informed that information about them may be passed on for these purposes.

Drugs and Alcohol Treatment groups

These types of groups may share information to help in the management of treatment services. The sharing of information on individuals involved in drugs and alcohol treatment requires their written consent for information about them to be shared with partner agencies. This is usually obtained when the individual commences treatment and is reviewed on an annual basis or at each treatment episode. It is rare that consent is not given, but when it is refused, each case should be considered on its individual merits, in line with the Data Protection Act and the Crime and Disorder Act, that is, information should be shared when there is a substantial chance that not sharing the data would be likely to prejudice the prevention or detection of crime and/or the apprehension of offenders.

Anti-Social Behaviour (ASB) Panels

Most CSPs operate ASB panels or some other form of ASB group that is responsible for deciding on ASB Orders (ASBOs), Acceptable Behaviour Contracts (ABCs) and Acceptable Behaviour Agreements (ABAs). These are multi-agency groups that make an assessment on individuals who are engaged in anti-social behaviour. Agencies usually included are the police, local council (including representatives from housing and education), Probation, Youth Offending Service, Fire and Rescue Service and health partners. These assessments require the backgrounds and actions of individuals who are referred to the panel to be examined and for this information to be shared amongst these agencies in accordance with the law. Any agencies that contribute to the panel can make a referral. Information can include:

- Name, date of birth and address of the perpetrator
- History of offences and behaviour
- Previous terms of custody, community orders and other supervision
- Probation OASys or YOIS assessment
- Drug and alcohol use
- Drug and alcohol treatment services

3.1.1.2 Information sharing to support the generation of CSP intelligence

There are certain sources of information that should be shared regularly and routinely by CSPs to assist the production of strategic assessments, problem profiles and other CSP intelligence. While the core datasets may differ between CSPs, Table 1 lists what are considered to be the most common core datasets. The content of each of these datasets is described in section 3.2.

Table 1. Core datasets for CSP information sharing

Core datasets to support the generation of CSP intelligence products – personalised and depersonalised information required on a regular and routine basis. Each dataset is listed with reference to whether the data shared should be shared on a depersonalised or personalised basis. Depersonalised information can be appended to an existing archive of previously sourced data. Personalised data records can be stored electronically but are subject to the legal conditions explained in Section 2.4	
Depersonalised	**Personalised**
• Police recorded crime – including details on the offence, the offender/accused and the victim or property targeted • Police disorder incident records • Council – recorded anti-social behaviour and environmental crime records • Fire and Rescue Service deliberate fires, malicious calls and assaults on staff • Probation OASYs assessments • Youth Offending Service YOIS assessments • Community surveys, e.g. Place Surveys, Face the People consultations, neighbourhood policing community consultations	• Prolific and Priority Offenders

Police crime data on the offender/accused and the victim/target (where recorded) are required as well as information on the offence in order to ensure a problem-oriented approach to the generation of intelligence products. The sharing of this information is vital in order to support partnership analysis of offending behaviour, prolificness of offending, risk factors associated with offending, detection, and reoffending; and to support the analysis of vulnerable groups, vulnerable targets (that is, property and products) and risk from further victimisation.

Over time, new datasets will be created. These may include refinements or updates to existing data (for example, an updated offender assessment system) or data that have been designed for a particular purpose (for example, to better understand public confidence). CSPs should ensure they are aware of new datasets and how they can be used.

3.1.2 Peripheral data

Peripheral data, while important for particular CSP intelligence requirements, do not need the same regular and routine updating as core datasets. Instead, these data are more normally shared as and when they are required to support a specific CSP intelligence requirement and are most usually applicable to the generation of intelligence products. Table 2 provides details of peripheral datasets. This list is not exhaustive but contains the datasets most commonly used in CSPs to support intelligence development.

Admissions to hospitals for injuries sustained from assaults are an increasingly important source of data to help CSPs understand violent crime. However, most areas in England and Wales have yet to adopt a routine process to improve the recording and sharing of this information by Accident and Emergency (A & E) departments, and until this has been done it is impractical to elevate it to a national core dataset. (The College of Emergency Medicine's *Guideline for Information Sharing to Reduce Community Violence*, available at www.collemergencymed.ac.uk/cem, contains advice for emergency departments on data sharing with CSPs.) Details on the minimum dataset for this information are given in Section 3.2. In those areas where these data are recorded by A & E departments, CSPs should elevate this dataset to 'core' status.

The data sharing pages of the Department of Health website (www.dh.gov.uk) contain useful advice and guidance, in particular on the A&E Serious Youth Violence Initiative.

Table 2. Peripheral datasets for CSP information sharing

Peripheral datasets – data that is required on a less routine basis to support particular CSP intelligence requirements.	
Depersonalised	**Personalised**
• Drug treatment records • Admissions to hospital A & E departments for injuries sustained from an assault • Admissions to hospital for drugs or alcohol related harm • Ambulance Service calls for service • Crimes on overground trains or at stations • Incidents on local trains, trams and stations • Incidents on local buses • School exclusions • Police stop and search • Police recorded results of drug tests for trigger offences • Police recorded detection status of offence	• Primary Care Trust Local Health Board data on alcohol and drugs misuse • Prison releases • Young Offenders' Institution releases • Environment Agency environmental crime

Voluntary and community organisations, and the business sector, can also provide a wealth of information to aid CSPs. However, as the set-up and data recording arrangements of these organisations are not consistent nationwide, we do not go into depth in this guidance on the data they may hold and what should be sourced from them. Instead we list some of the groups that may exist locally and the type of information they hold that could be of use:

- domestic violence – this information is usually reported through MARAC, but groups that support victims of domestic abuse may hold additional information that can be of use
- homelessness and rough sleepers – information on victims of homelessness, alcohol and drugs misuse, and the crime/ASB/abuse they may have suffered

- business/retail groups – information on prolific shoplifters
- gay and lesbian support groups – information on homophobic abuse and other hate crime
- religious groups – information on abuse and hate crime

Information on enforcement, prevention and reassurance initiatives should also be shared. This can include information about street lighting improvements, the location and coverage of CCTV cameras, Neighbourhood Watch, police operations, burglary prevention schemes (e.g Smartwater, window locks, alleygating), youth provision, and the location of targeted patrols. In addition, data on the location of public services (e.g. schools, youth centres, neighbourhood offices, and transport facilities such as bus stops) can also aid analysis. We do not list all these information types in this guidance, but these types of information should be shared as a matter of routine with relevant partners. In any situation where the information can be considered as personal (e.g. proactive targeting of a prolific offender) then the legal basis for sharing this information must be considered.

3.2 MINIMUM DATASETS FOR CSPS

In this section we describe the datasets that should be shared within a CSP to support the generation of intelligence products; they can also help support many operational business processes in a CSP (other than those described in 3.1.1.1) – this may include using these data to identify a new spate of incidents and emerging problems, and sharing data with neighbourhood practitioners. The minimum datasets refer to those listed in Tables 1 and 2 as core or peripheral datasets. In this section we describe the source and the recommended minimum dataset (i.e. the datafields) that should be shared. We also describe the type of data that should be shared – personal or depersonalised.

Datasets labelled depersonalised most usually require some processing to ensure they cannot be used in any way to identify an individual. This includes the removal of an individual's name from the original (personal) data record, but may also require some processing of the recorded address. A process for depersonalising an address, but that retains a high level of geographical resolution in the data record is described in Appendix 1. In summary, this process involves removing the house number or name, but allowing postcode-level address information (such as the street name, full postcode and locality) to be shared (on the basis that there are at least four properties within that postcode). Datasets labelled in this section as 'depersonalised' therefore refer to a depersonalised version of the original record, and list datafields that are allowed to be shared. For example, if the dataset is described as depersonalised and includes a datafield containing address or location information, it is the depersonalised version of this address/location that is allowed to be shared.

We also list other sources of data that are available in aggregate format to support the development of intelligence.

Many of the minimum datasets list Easting and Northing geographic coordinates as datafields. Not all partner agencies are able to provide these geographic coordinates. Please refer to Appendix 1 for details on how Easting and Northing coordinates can be determined and the necessary processes required for depersonalising these geographic references.

3.2.1 Police recorded crime (depersonalised data)

- ***Source:*** Local police force
- ***Type of data:*** Recorded offences of crime, including details on the offence, the accused/offender and the victim or target (e.g. a building or other form of property such as a car)

- ***Recommended minimum dataset*** (it is recommended that these data are provided as three separate files):

  Datafields on the offence

  - Crime reference number
  - Type of offence – Home Office classification code
  - Committed from date
  - Committed from time
  - Committed to date
  - Committed to time
  - Address/location of offence
  - Easting coordinate (relating to the address/location where the offence occurred)
  - Northing coordinate (relating to the address/location where the offence occurred)
  - Method of entry
  - Property stolen
  - Use of a weapon (e.g. describing type of weapon or part of body used if applicable in committing the offence)
  - Marker/flag for distraction burglary
  - Marker/flag for drugs-related incident
  - Marker/flag for alcohol-related incident
  - Marker/flag for racially-motivated incident
  - Marker/flag for domestic incident

  Datafields on the offender/accused

  - Crime reference number
  - Offender reference number
  - Gender
  - Age (or date of birth)
  - Ethnicity
  - Occupation
  - Address/location of offender – address is the offender's primary address
  - Easting coordinate (relating to the home address of the offender/accused)
  - Northing coordinate (relating to the home address of the offender/accused)

Datafields on the victim

- Crime reference number
- Gender
- Age (or date of birth)
- Ethnicity
- Association with offender (e.g. husband, wife, ex-partner, friend, stranger)
- Occupation
- Address of victim
- Easting coordinate (relating to the home address of the victim)
- Northing coordinate (relating to the home address of the victim)

It is important that police forces not only share information on the offence, but also information on the offender/accused and the victim. Offender and victim data are vital in order to develop a problem-oriented approach – this highlights that information not only on the offence, but also on the offender and the victim (or target, e.g. building or vehicle) is vital if the problem is to be properly understood. Some police forces may question the reliability of the information that they have recorded but often this is the best, if not only, source of information for exploring these components of a crime problem. In this case, something rather than nothing is the best philosophy to adopt, with the opportunity to use metadata (see Section 3.4) as a means to record any caveats or conditions on the use of this information. The supply of this information is legally permissible and can be vital in helping the CSP in its analysis of offending behaviour, prolificness of offending, risk factors associated with offending, detection and re-offending; and support the analysis of vulnerable groups, vulnerable targets (i.e. property and products) and risk from further victimisation.

The sharing of the crime reference number in each of the three recorded crime datasets facilitates the opportunity to link these data and explore additional features of interest, for example, linking the details of the offence to the victim data helps to identify where people of a certain age experience high levels of victimisation.

3.2.2 Police incident records (depersonalised data)

- ***Source:*** Local police force
- ***Type of data:*** Calls for police service, including recorded incidents of disorder and domestic incidents. These recorded incidents refer to domestic incidents, street disorder such as rowdy and nuisance behaviour, street drinking, vehicle nuisance and other anti-social incidents such as hoax calls
- ***Recommended minimum dataset:***
  - Incident reference number
  - Type of incident
  - Marker/flag for domestic incident
  - Date of incident
  - Time of incident

- Address/location of incident
- Easting coordinate (relating to the address/location where the incident occurred)
- Northing coordinate (relating to the address/location where the incident occurred)

3.2.3 Council-recorded incidents of ASB and environmental crime (depersonalised data)

- ***Source***: Local council. In some areas local housing associations also record this information and should be additionally sourced.
- ***Type of data***: Recorded incidents of ASB and environmental crime reported to the council. These recorded incidents most commonly refer to neighbour noise nuisance, rowdy behaviour, nuisance caused by young people, graffiti, vandalism, flytipping, and abandoned vehicles. Flytipping incidents refer to domestic or small scale dumping of non-domestic waste recorded for the purpose of completing 'FlyCapture' returns to the Environment Agency
- ***Recommended minimum dataset:***
  - Incident reference number
  - Type of incident
  - Date of incident
  - Time of incident
  - Value of property damaged (graffiti and vandalism incidents)
  - Size or weight of waste that is dumped (flytipping)
  - Make, model, and age of vehicle (abandoned vehicles)
  - Registered address of vehicle (abandoned vehicles)
  - Address/location of incident
  - Easting coordinate (relating to the address/location where the incident occurred)
  - Northing coordinate (relating to the address/location where the incident occurred)

3.2.4 Fire and Rescue Service deliberate fires, malicious calls and assaults on staff (depersonalised)

- ***Source:*** Local Fire and Rescue Service
- ***Type of data:*** recorded incidents of deliberate fires (including fires to property – primary fires, and fires at other sites such as waste containers – secondary fires), malicious calls and assaults on staff
- ***Recommended minimum dataset:***
  - Incident reference number
  - Type of incident
  - Date of incident
  - Time of incident
  - Number of casualties (where relevant)
  - Address/location of incident

- Easting coordinate (relating to the address/location where the incident occurred)
- Northing coordinate (relating to the address/location where the incident occurred)

3.2.5 Probation OASys assessments (depersonalised data)

- ***Source:*** Local Probation Trust
- ***Type of data:*** Records on Probation clients, describing the assessment of their offending in terms of their needs and future risks
- ***Recommended minimum dataset:***
  - Client reference number
  - Age
  - Gender
  - Postcode (full postcode)
  - Offence description
  - Emotional wellbeing link to offending (LTO)
  - Thinking and behaviour LTO
  - Attitudes LTO
  - Accommodation LTO
  - Employment, training and education LTO
  - Financial management LTO
  - Relationships
  - Lifestyle and associations LTO
  - Drug misuse LTO
  - Alcohol misuse LTO
  - Date assessment was completed
  - Risk of reconviction: high, medium, low
  - Risk of harm to others
  - Number of months planned for supervision

3.2.6 Youth Offending Service (YOS) assessments (depersonalised data)

- ***Source:*** Local Youth Offending Service
- ***Type of data:*** Records on YOS clients, describing the assessment of the offender in terms of their needs and future risks
- ***Recommended minimum dataset:***
  - Client reference number
  - Age
  - Gender

- Postcode (full postcode)
- Offence description
- Marker/flag for persistent offender
- Date of assessment
- Ratings for each category of risk assessment (14 categories associated with the risk of reoffending. Two ratings relate to risk of harm and vulnerability)

3.2.7 Prolific and other Priority Offenders (sensitive personalised data)

- ***Source:*** Local police force
- ***Type of data:*** Records on PPOs in order to keep account of their activities and status
- ***Recommended minimum dataset:***
  - Offender reference number
  - Name
  - Gender
  - Age (or date of birth)
  - Ethnicity
  - Occupation
  - Offences committed
  - Current status (e.g. in custody, subject to proactive targeting by the police, subject only to basic monitoring)
  - Address/location of offender – address is the offender's primary address
  - Easting coordinate (relating to the home address of the offender/accused)
  - Northing coordinate (relating to the home address of the offender/accused)

3.2.8 Prison releases (personalised data)

- ***Source:*** National Offender Management Service
- ***Type of data:*** Records on prisoners who reside in the local area, with details on when they are to be released
- ***Recommended minimum dataset:***
  - Name
  - Gender
  - Date of birth
  - Length of sentence
  - Offence committed
  - Address where they will reside after release
  - Easting coordinate (relating to the address where they will reside after release)
  - Northing coordinate (relating to the address where they will reside after release)

3.2.9 Young Offender Institution releases (personalised data)

- ***Source:*** Young Offender Institutions
- ***Type of data:*** Records on young offenders who reside in the local area, with details on when they are to be released
- ***Recommended minimum dataset:***
  - Name
  - Gender
  - Date of birth
  - Length of sentence
  - Offence committed
  - Address where they will reside after release
  - Easting coordinate (relating to the address where they will reside after release)
  - Northing coordinate (relating to the address where they will reside after release)

3.2.10 Drug treatment – adults (depersonalised data)

- ***Source:*** Drug and Alcohol Action Team
- ***Type of data:*** Records on adults in drug treatment (recorded on the National Drug Treatment Service Management System), either self referred, or via the Criminal Justice System or the Drug Interventions Programme (DIP)
- ***Recommended minimum dataset:***
  - Client reference number
  - Age
  - Gender
  - Postcode (full postcode)
  - Primary drug of use
  - Secondary drug of use
  - Referral source
  - Type of treatment
  - Date when treatment began
  - Planned discharge date

3.2.11 Drug treatment – young people (depersonalised data)

- ***Source:*** Drug and Alcohol Action Team
- ***Type of data:*** Records on young people in drug treatment (recorded on the National Drug Treatment Service Management System), either self referred, or via the Criminal Justice System or the Drug Interventions Programme
- ***Recommended minimum dataset:***
  - Client reference number
  - Age
  - Gender
  - Postcode (full postcode)
  - Primary drug of use (includes alcohol)
  - Secondary drug of use
  - Referral source
  - Type of treatment
  - Date when treatment began
  - Planned discharge date

3.2.12 Admissions to Accident and Emergency (A & E) departments for injuries sustained from an assault (depersonalised data)

- ***Source:*** Hospital A & E department, or Primary Care Trust/Local Health Board
- ***Type of data:*** Records on patients admitted due to injuries sustained from an assault
- ***Recommended minimum dataset:***
  - Patient reference number
  - Age
  - Gender
  - Ethnicity
  - Address of patient

  The datafields listed above are recorded by A & E departments when the patient presents him/herself.

  The data listed below may not be recorded by the A & E department but attempts should be made to record it to help understand issues associated with assaults:

  - Type of incident – assault
  - Date of incident
  - Time of incident

- Type of location where incident took place: at home; in a licensed premise; outside a licensed premise; on the street; other (please state)
- Location where incident took place: street name; premise name; other (please state) or additional location information (e.g. junction with other street, taxi rank)
- Easting coordinate (relating to the address/location where the assault occurred)
- Northing coordinate (relating to the address/location where the assault occurred)
- Whether reported to the police

3.2.13 Admissions to hospital for drugs and alcohol related harm (depersonalised data)

- ***Source:*** Primary Care Trust/Local Health Board
- ***Type of data:*** Records on patients admitted due to drugs- or alcohol-related harm, including drug overdose or drug/alcohol misuse
- ***Recommended minimum dataset:***
  - Patient reference number
  - Age
  - Gender
  - Ethnicity
  - Postcode (full postcode)
  - Reason for admission/diagnosis

3.2.14 Ambulance Service calls for service (depersonalised)

- ***Source:*** Hospital A & E department, or Primary Care Trust/Local Health Board
- ***Type of data:*** Records on patients that required an ambulance
- ***Recommended minimum dataset:***
  - Patient reference number
  - Age
  - Gender
  - Ethnicity
  - Address of patient
  - Type of incident
  - Date of incident
  - Time of incident
  - Address/location where incident took place
  - Easting coordinate (relating to the address/location where the incident occurred)
  - Northing coordinate (relating to the address/location where the incident occurred)

3.2.15 Crimes on overground trains or at stations (depersonalised)

- ***Source:*** British Transport Police[4]
- ***Type of data:*** Records on offences committed on trains or at stations
- ***Recommended minimum dataset:***
  - Crime reference number
  - Type of offence
  - Date of incident
  - Time of incident
  - Address/location of offence or route on which offence occurred
  - Easting coordinate (relating to the address/location where the offence occurred)
  - Northing coordinate (relating to the address/location where the offence occurred)
  - Offender gender
  - Offender age (or date of birth)
  - Offender ethnicity
  - Victim gender
  - Victim age (or date of birth)
  - Victim ethnicity

3.2.16 Incidents on local trains/trams and stations (depersonalised data)

- ***Source:*** Local transport provider (e.g. Transport for London, Greater Manchester Passenger Transport Executive, NEXUS)[4]
- ***Type of data:*** Records on incidents committed on the transport network, if recorded separately from local police force incidents and British Transport Police
- ***Recommended minimum dataset:***
  - Crime reference number
  - Type of offence
  - Date of incident
  - Time of incident
  - Address/location of offence or route on which offence occurred
  - Easting coordinates (relating to the address/location where the offence occurred)
  - Northing coordinates (relating to the address/location where the offence occurred)
  - Offender gender
  - Offender age (or date of birth)

[4] Please see the Department of Transport's guidance entitled *Crime on Public Transport – Guidance for Community Safety Partnerships in England and Wales*, available at www.crimereduction.homeoffice.gov.uk/crimereduction056.htm

- Offender ethnicity
- Victim gender
- Victim age (or date of birth)
- Victim ethnicity

3.2.17 Incidents on local buses (depersonalised data)

- ***Source:*** Local public bus transport provider[4]
- ***Type of data:*** Records on incidents committed on buses, if recorded separately from local police force incidents
- ***Recommended minimum dataset:***
  - Crime reference number
  - Type of offence
  - Date of incident
  - Time of incident
  - Address/location of offence or route on which offence occurred
  - Easting coordinate (relating to the address/location where the offence occurred)
  - Northing coordinate (relating to the address/location where the offence occurred)
  - Offender gender
  - Offender age (or date of birth)
  - Offender ethnicity
  - Victim gender
  - Victim age (or date of birth)
  - Victim ethnicity

3.2.18 School exclusions (depersonalised data)

- ***Source:*** Local council
- ***Type of data:*** Records on pupils excluded from school
- ***Recommended minimum dataset:***
  - Gender
  - Age
  - Ethnicity
  - Name of school
  - Easting coordinate (relating to the school address)

[4] Please see the Department of Transport's guidance entitled *Crime on Public Transport – Guidance for Community Safety Partnerships in England and Wales*, available at www.crimereduction.homeoffice.gov.uk/crimereduction056.htm

- Northing coordinate (relating to the school address)
- Type of exclusion (e.g. permanent, temporary)

3.2.19 Environment Agency recorded environmental crime (personalised data)

- ***Source:*** Environment Agency
- ***Type of data:*** Records on environmental crime including the illegal dumping of waste and illegal waste processing sites. Local councils record flytipping on FlyCapture but large dumps of waste are passed directly to the Environment Agency. Large flytips and illegal waste processing sites usually handle tyres and construction waste, and there is evidence suggesting links between this type of activity and organised crime
- ***Recommended minimum datasets:***

A. Illegal dumping of waste (personalised)

(Large illegal dumps that are recorded separately to small flytipping incidents that are recorded on FlyCapture by local councils. That dataset is described as personalised because full address/location information is allowed to be shared.)

- Incident reference number
- Type of incident (e.g. construction waste, tyres)
- Committed from date of incident
- Committed from time of incident
- Committed to date of incident
- Committed to time of incident
- Address/location of incident
- Easting coordinate (relating to the address/location where the incident occurred)
- Northing coordinate (relating to the address/location where the incident occurred)

B. Illegal waste processing sites (personalised)

- Site reference number
- Name of waste processing site
- Name of site owner
- Type of illegal waste
- Date identified
- Address of site
- Easting coordinate (relating to the address of the site)
- Northing coordinate (relating to the address of the site)

3.2.20 Police recorded stop and search (depersonalised data)

- ***Source:*** Local police force
- ***Type of data:*** Recorded stops and searches. A stop may not result in a search, but as a minimum details of the search rather than all stops that do not result in a search should be shared
- ***Recommended minimum dataset:***
  - Reference number
  - Date of search
  - Time of search
  - Gender of suspect
  - Age of suspect
  - Ethnicity of suspect
  - Reason for search e.g. drugs, carrying a weapon, in possession of stolen goods
  - Results of search e.g. arrest, caution, no action
  - Address/location of search
  - Easting coordinate (relating to the address/location of the search)
  - Northing coordinate (relating to the address/location of the search)

Stop and search data are useful for exploring patterns and results generated from this type of activity, particularly when used as a tactic to try to address certain crime issues (e.g. young people carrying knives).

3.2.21 Police recorded results of drug tests for trigger offences (depersonalised data)

- ***Source:*** Local police force
- ***Type of data:*** Trigger offences are types of offences that are most usually influenced by drug misuse. A number of police forces in England and Wales are Intensive DIP areas, where there is a mandatory requirement for testing for drugs for these types of offences.
- ***Recommended minimum dataset:***
  - Crime reference number
  - Type of offence – Home Office classification code
  - Result of drugs test
  - Type of drug used

Drug test results for trigger offences can be useful to help understand the level of drug use in the community and the direct impact that it has on crime.

3.2.22 Police recorded detection status of offence (depersonalised data)

- ***Source:*** Local police force
- ***Type of data:*** Status on the detection of a recorded criminal offence. This can be used to help identify the types of crime that are difficult to detect and performance changes in detection levels.
- ***Recommended minimum dataset***
  - Crime reference number
  - Type of offence – Home Office classification code
  - Detection status

3.3 DATA AVAILABLE IN AGGREGATE FORM

There are several sources of information that provide aggregate data and that are complementary to personalised and depersonalised data, particularly for the development of intelligence products. This section provides a summary of this information.

If the information is not in the public domain then all the information that is listed can be accessed via authorised means in the CSP (and should therefore be treated as 'restricted'. Data that should be treated as restricted are marked accordingly in this section). Consult your CSP Coordinator for details on accessing this information.

3.3.1 iQUANTA (RESTRICTED)

Source: Home Office

iQuanta provides a rich source of information that CSPs can access to support performance monitoring. The data that can be sourced is aggregate information that can allow CSPs to monitor trends in crime, including how they are performing in relation to their most similar CSPs. Data on the British Crime Survey can also be accessed from iQuanta to help CSPs monitor levels and changes in public perceptions and satisfaction with the service that the police and other local agencies provide for tackling crime and anti-social behaviour.
(http://police.homeoffice.gov.uk/performance-and-measurement/iquanta/index.html)

3.3.2 Ffynnon – the pan-Wales performance management system (RESTRICTED)

Source: Welsh Assembly

Ffynnon is an organisational performance management system that allows users to collate and present information about risks, projects and performance indicators by using a range of visual representations. This engages the user and helps them to understand what is often quite complex data. In addition, Ffynnon allows users to benchmark their performance against that of others.
(http://wales.gov.uk/topics/localgovernment/ffynnon/?lang=en)

3.3.3 Place Surveys

Source: Local council

The Place Survey provides information on people's perceptions of their local area and the local services they receive. The Place Survey is carried out every two years in each local government area and asks several questions that are directly relevant to community safety. These are:

- How safe or unsafe do you feel when outside in your local area after dark?
- How safe or unsafe do you feel when outside in your local area during the day?
- Thinking about this local area, how much of a problem do you think each of the following are: noisy neighbours or loud parties; teenagers hanging around the streets; rubbish or litter lying around; vandalism, graffiti and other deliberate damage to property or vehicles; people using or dealing drugs; people being drunk or rowdy in public places; abandoned or burnt-out cars?
- How satisfied or dissatisfied are you with each of the following public services in your local area: local police force, local fire and rescue service?
- How much would you agree or disagree that the police and other local public services seek people's views about these issues in your local area?
- How much would you agree or disagree that the police and other local public services are dealing successfully with these issues in your local area?

The first Place Surveys were conducted in 2008/09. Prior to this, similar information was available in the 2006 Local Government User Satisfaction Survey (LGUSS) and the 2005/06 Best Value Performance Indicators (BVPIs) and can be sourced to offer some opportunity for comparisons and trends over time.

3.3.4 Face the People information

Source: Community safety team

Face the People sessions involve senior representatives of the CSP meeting the public and can generate useful information that helps identify perceptions, concerns, worries and priorities.

3.3.5 Neighbourhood Policing community consultations

Source: Local police force

Neighbourhood Policing teams regularly carry out surveys that can generate useful information on local concerns and priorities for community safety.

3.3.6 TellUs Survey

Source: Local council

This is a survey of children and young people across England, asking their views about their local area, and including questions that relate to personal safety. The survey is repeated annually, with results being available in the spring of each year (www.tellussurvey.org.uk).

It is important that any findings from survey data are assessed for their quality and reliability, and supported with information on how they should be used (see also section 3.4 on metadata).

3.3.7 Prolific and other Priority Offender cohort (RESTRICTED)

Source: Home Office

National Indicator 30 data (re-conviction rate of PPOs). This data is provided quarterly to show areas their performance in reducing the conviction rate of identified PPOs in their areas.

PPO Scheme Performance Framework data is a collation of information that is updated every three months from JTrack, the Police National Computer and returns from local PPO schemes to provide headline measures for a cohort of PPOs. These data can be used to explore the numbers of PPOs in each police force, demographic details, recent offences and convictions, results of drug testing, alcohol misuse, their current status, and levels of re-offending. The data can be accessed via authorised means within the CSP.

3.3.8 DIRWeb (RESTRICTED)

Source: Home Office

This information can be used for monitoring engagement on the Drug Interventions Programme (DIP). A Drug Intervention Record (DIR) form is completed every time a client is assessed by the DIP programme. This information can show a client's journey through DIP including their engagement, treatment and transfers. It also includes demographic profiles of those on the programme. (www.dirweb.co.uk)

3.3.9 Admissions for drugs and alcohol misuse

Source: Public health observatories

The public health observatories collate information that relates to drugs and alcohol misuse, including data extracted from the National Drug Treatment Management System (NDTMS) and hospital admissions. Each public health observatory publishes aggregated information online at www.apho.org.uk

3.3.10 Drug and alcohol use and treatment (RESTRICTED)

Source: Drug and Alcohol Action Team (DAAT)

The Drugs and Alcohol Needs Assessment is a report produced by each DAAT annually and it can provide a rich source of aggregate information on drugs and alcohol use and treatment. This includes details on the following:

- the number of problematic drug misusers, including an assessment based on those that are known about and the estimates that are generated annually for the DAAT. This can then help to assess the penetration of drug treatment services.
- drug use of choice
- referral route to drug treatment (e.g. self referral, via the CJS or DIP)
- demographic profile of those in treatment
- employment status of those in treatment
- home residence of those in treatment
- length of time in treatment. This measure is useful as drug treatment is more likely to be effective if clients are retained in treatment for 12 weeks or more.
- discharges from drug treatment for those that are now drug free. Treatment services can tend to focus on increasing numbers, and retaining clients in treatment whilst reducing risks to their health and the wider impact on society. This type of data can be useful for exploring further the effectiveness of drug treatment by measuring the numbers of users discharged from treatment that are drug free.

3.3.11 Violent extremism and terrorism (RESTRICTED)

Source: Local police force

Intelligence captured in the local PREVENT Strategic Assessment should be shared with the CSP. As a minimum this should include

- The current local threat
- Known levels of violent extremism in the local area
- Details on vulnerable persons, groups, communities and places that may be exploited by violent extremism

Low-level crime and ASB, and violent extremism and terrorism are at opposite ends from each other on the public safety severity spectrum, however the continuum that runs through them is that they affect communities, and that offenders and perpetrators come from local communities. Often it is the most marginalized and fragmented communities that are at the greatest risk of high levels of crime, and these communities are also the ones where resilience needs strengthening to help counter the global terrorist ideology. Hence, considering community safety alongside the PREVENT agenda is practical for addressing these wide-ranging, but community-based, public safety issues.

3.3.12 Census of Population

Source: Office for National Statistics or local council

Data from the Census can be sourced either online or from the local council. This data provides a rich source of demographic and socio-economic information including data by age group, gender, ethnicity, educational attainment, occupation, housing tenure and housing type.

3.3.13 Neighbourhood Statistics

Source: The Neighbourhood Statistics Service (NeSS)

NeSS provides free access to aggregate government administrative information including data on welfare benefits (such as income support), public access to services (such as access to pharmacies and schools), lifestyle groups, population movement and migration, and unemployment. (www.neighbourhood.statistics.gov.uk)

3.3.14 Index of Deprivation

Source: Communities and Local Government

The Index of Multiple Deprivation combines a number of indicators, chosen to cover a range of economic, social and housing issues, into a single deprivation score for each small area in England. It provides a score for each area and a rank, allowing areas to be compared with one another according to their level of deprivation. It is updated approximately every four years and provides data at local authority level and for each Lower Super Output Area in England. (www.communities.gov.uk/communities/neighbourhoodrenewal/deprivation/deprivation07/)

In Wales, the equivalent index (the Welsh Index of Multiple Deprivation) is available from the Welsh Assembly website at: http://wales.gov.uk/topics/statistics/theme/wimd/?lang=en

3.3.15 Major housing, retail and other construction developments

Source: Local council

Major construction developments, including large-scale regeneration projects, can have a sizeable positive or negative impact on community safety. It is useful to consult on this information periodically to identify the possible impact that these large-scale activities may have. This type of information can be sourced from the local council planning department

3.3.16 Calendar of public and community events and festivities

Source: Local council

Public events, community events and festivities can have an impact on community safety. It is useful to consult on this information periodically to identify the possible impact that these activities may have. This type of information can be sourced from the local council's culture and leisure department.

3.4 METADATA

Metadata is information about information and provides the means to record details about what a dataset contains and any caveats and conditions on its use. It is recommended that metadata is provided with each supply of data used for the generation of intelligence products, or, in the case of core data, that the metadata recorded with the first supply of data is kept up to date. The following metadata should be provided:

- Name of agency supplying the information
- Name and contact details of supplier
- Dataset name
- Time period covered
- File format
- Number of records supplied
- Date supplied
- List of datafields contained in the dataset
- Explanation of datafields contained in the dataset if the field is not self-explanatory from its datafield name
- Caveats and considerations on the use of the dataset

There are occasions when certain caveats and conditions of use should be applied to data. For example, this could relate to when the completeness of certain datafields is questionable, but their inclusion can be informative. To ensure that appropriate care is taken with their use in intelligence products, the information supplier should be in a position to record these caveats and terms of use to ensure that data are not used inappropriately.

A metadata form with the above details can also be a useful place to remind the agency to whom data is being supplied what their legal roles and responsibilities are, ensuring that the data are processed in accordance with the ISP, and that there still remain restrictions on the use of the information even if it is depersonalised. This includes ensuring that any use of the information in intelligence products requires these products to be marked as 'restricted'.

It is also important to establish from the outset if any particular coding systems are used in the dataset (e.g. numerical coding used for ethnic groups) and what methodology has been used to determine any geographic coordinates included as datafields in the dataset.

4. How to share information

In this section we describe how information should be shared. We begin by describing many of the common barriers to information sharing then set out five key principles that help overcome these difficulties and promote good information sharing. We then add to this by explaining the processes involved in information sharing and how, by drawing from practice, a number of steps can be followed to help facilitate good practice in sharing information. We summarise this with a flow model that helps to illustrate the direction to follow and questions to consider when sharing information. Answering these questions should be possible by drawing from this and other sections of the guide. We finish this section by describing an information-sharing framework that can facilitate these processes and support the effective and efficient sharing of information.

4.1 BARRIERS TO INFORMATION SHARING

Many CSPs have experienced difficulties and barriers to information sharing. Issues with information sharing have been well-rehearsed and documented in other publications (see Radburn, 2000; Cabinet Office, 2000) so we avoid going into great depth here. Many CSPs often experience difficulties in information sharing because they operate an ad hoc data exchange arrangement, which in turn results in the information sourced being too little and too late for it to be of any real use.

The lack of any routine and the lack of defined processes for sharing information between CSP partners can create a number of problems:

- There is a lack of consistency in the type of information that is requested, meaning that information suppliers perform new processes each time a request is made. This has an obvious time demand that may result in partners not sharing information (i.e. they claim they do not have the time to meet the request) or affects how quickly a request can be met.
- The over-reliance on one partner providing information can create stresses and tensions in an information-sharing relationship, particularly when the information supplier receives little in return.
- The information that is exchanged exists only in the form of reports containing statistics, rather than raw data. Whilst individual partners may perform analysis on their own data, the lack of sharing of raw data can prevent the types of multi-agency data analysis that the CSP, in part, was designed to do.

Other barriers to information sharing include:

- a lack of resources and skills in bringing partnership information together;
- the silo mentality – 'it's our data and you are not using it' – continues to act as one of the main barriers to information sharing;
- agencies charging for their data. This has happened on several occasions when agencies have contracted a service out, and when a request for data from the CSP is made to that contracted service, they are unwilling to provide the information without levying some charge for its supply;
- exchanging data can make those who originally shared the data nervous about how it will be used and what results will come from analyses, especially if data are used in a manner that is slightly different from how the agency itself may use these data. This nervousness may then result in them trying to avoid sharing information;

- agencies may use the excuse that they do not think their data is of good quality, so restrict access to it, particularly because they think others may use the data inappropriately and without recognising its flaws;
- where the legal basis permits the sharing of personal data, these laws are often not well understood by practitioners. These practitioners may then think that sharing the data will break the law, therefore refuse access to data, rather than adopting a 'can do' attitude and working through the confusion;
- the processing requirement to depersonalise data can be resource intensive. Because a time resource is required to depersonalise data, the excuse often given is that people do not have the time to carry out this duty – therefore access to data is denied;
- poor communication between the 'right' people in agencies will often fail to break down the communication barriers in a partnership, and frustrate access to information; and
- the lack of a co-ordinated approach to information sharing often results in poor information management and little opportunity for strategic information improvements to information-sharing arrangements and data quality.

Information sharing requires careful nurturing. Not all the challenges will be solved in one go. Lack of awareness or cultural barriers require examples to illustrate how information sharing – to the level of precision required and in compliance with any legislation – is practical and cost effective, applies proportional effort to the benefits gained, improves CSP decision-making, and brings returns on investment, such as helping to achieve a reduction in crime. In the next sections we set out some principles and guidance on how best to go about information sharing in a manner that helps to overcome and avoid these barriers.

4.2 PRINCIPLES OF INFORMATION SHARING

There are five key principles that should be considered when sharing information in a CSP. Following these principles will help to ensure that information shared is put to practical use, so partners who provide information are clear about, and comfortable with, how information will be shared and used.

4.2.1 Principle 1: Explain why the information will help the CSP

It is vital that any information is shared so that it can contribute to the service delivery of the CSP. Explaining why the information will be of use needs to be done by describing the questions that this information will help answer and how the information will be used. This helps to explain that the information will be of value and overcome concerns that the information will be used inappropriately.

4.2.2 Principle 2: Identify the potential benefits for the information supplier

Any agency that is sharing information is doing so with some resource cost. To help them to justify this cost (beyond it being for the general good of the CSP) it is useful to identify the potential benefits for the information supplier that will come from sharing this information. This may include them being able to receive other partner agency information or helping them make improvements in their service delivery as a result of the way in which information is used. Most often the collation of different partner agency information is greater than the sum of its parts in helping to understand a problem. In addition, other agencies may be able to use their expertise to analyse information in ways that had not been previously considered, or were not achievable because analytical resources in the agency from which the information was sourced are limited.

4.2.3 Principle 3: Information shared must be fit for purpose

Information shared needs to be fit for the purpose of its use. Fitness for purpose with regards to sharing information for community safety is defined in terms of two key qualities – the first quality ensures that all information sharing is legal, with the second relating to the content of the information that is supplied.

- Compliance with legislation: there must be a clear legal basis for the sharing of information. This must be considered for both personal and depersonalised information to help ensure that data are shared in a manner that is compliant with legislation. The legal basis on which data can be shared then helps to define the other qualities.
- Content of information: the data shared must include the relevant datafields and these datafields need to contain the relevant information. The relevance of the information can be defined in four terms.
  - Precision: precision refers to the detail contained in a datafield. Information must be of a precision that helps the CSP to maximise its use. For example, if a CSP is exploring issues associated with the victimisation of young people, the data would be more fit for purpose if it allowed each one-year age group to be explored, rather than the age groups being aggregated together prior to their supply. If the data were aggregated into the groups 10–15, 15–20, 20–25, this would restrict the use of these data if the definition of a 'young person' for the purpose of understanding the problem was 17 years of age or under. Precision also refers to the geographical level at which data are shared. CSPs typically require data to be geographically precise to the sub-neighbourhood level (e.g. to at least the postcode unit level) to maximise its use. Information should be shared to its highest legally permissible level of precision.
  - Accuracy: accuracy refers to the deviation of information away from its true value. Information must be accurate for CSP purposes; however, there are occasions when the true value may not be known (e.g. the age of a person who committed an offence may not be exactly known because it relies upon a judgement by the victim or a witness). It is important that information suppliers make information users aware of any issues with accuracy. Issues with accuracy should not prevent the supply of information. Information is never perfect, and most often information accuracy improves subsequent to its use.
  - Completeness: a complete state is one that requires nothing to be added. Information shared for the purposes of community safety should be as complete as possible. When an information supplier has concerns about the completeness of information this should be specified in order to ensure that data users do not misinterpret the information. As with accuracy, issues of completeness should not prevent the supply of information. Often a particular source of information provides the only available information on that problem, and whilst it may not be complete, it at least provides something that can be used to help explore certain aspects of a problem.
  - Currency: data need to be timely to support CSP intelligence-led activities. Timeliness differs according to the use that data are put to. For example, data on a domestic violence incident may need to be shared amongst the partnership immediately after the incident to ensure that an appropriate response is put in place to help address any future risk. Crime data used for a problem profile may not need to be as timely, and could consist of data for the last 12 months, with the last record referring to the end of the previous month.

Measuring the fitness for purpose of information therefore requires the legal basis to be clear, with the qualities of its content to be considered against the use to which the information will be put. As long as the legal power exists to share information, other barriers should not stand in the way of sharing information to the required level of content.

4.2.4 Principle 4: Data are securely managed

Data used by a CSP should be managed within a secure environment. This includes the management of depersonalised information, which, while it does not identify an individual, can still be restricted information that only authorised users can access.

4.2.5 Principle 5: Data are easy to access

Data should be held in an environment where they are easy to access. Ease of access to data helps to promote their use and overcome the often time-consuming process of sourcing and extracting data.

In the next section we help illustrate how these principles can be applied in practice by describing the processes involved in information sharing.

4.3 PROCESSING INFORMATION-SHARING REQUIREMENTS

The process of sharing information requires certain steps to be taken. In this section we describe these various steps and illustrate how they can be carried out against the principles set out in previous sections of this guide. We also summarise these steps using the flow model shown in Figure 3 (see p. 59) which sets out how to handle the information required for performance monitoring tasks, the development of intelligence products, identifying new incidents and emerging problems, and for supporting the delivery of services to particular groups or individuals (as defined in Section 2.3). The flow model also captures in summarised form key pieces of information from previous sections.

4.3.1 Step 1: Identify the information that is required and establish the legal basis on which it can be shared

The first step involves identifying what the information will be used for and the types of questions it will answer:

- Will the information be used for
  - performance monitoring purposes?
  - an analytical task such as assisting in the development of an intelligence product?
  - a CSP business meeting?
- What types of questions should the information help to answer, for example:
  - How have levels and perceptions in ASB changed over the last year? (performance monitoring)
  - Why is violent crime increasing across the district? (development of intelligence products)
  - What progress has been made in the management of the district's PPOs? (CSP business meeting).

In some situations, one of the first requirements is to ensure that definitions are agreed in relation to the questions being asked. For example, what do we mean by ASB and violent crime in terms of ways that they can be measured? By 'violent crime', do we mean violent crime associated with the night-time economy or 'violent crime' in wider definitional terms?

For the purpose of developing intelligence products, particularly problem profiles, it is useful to pose certain hypotheses in relation to the problem that needs to be explored, because this helps to identify the information that is required. For example, in considering why violent crime associated with the night-time economy is increasing, the following hypotheses could be tested:

- the increase in violent crime is concentrated on certain places, days of the week and times of the day rather than a more widespread increase – data that could be used to test this hypothesis include police recorded crime data and admissions to A & E departments for assault
- the increase in violent crime is more associated with less serious violence rather than serious violence – data that could be used to test this hypothesis include police recorded crime data and admissions to A & E departments for assault
- the increase in violent crime is associated with a small number of licensed premises rather than a more general increase – data that could be used to test this hypothesis include police recorded crime data, admissions to A & E departments for assault, ambulance call-outs for violent offences and data on the location of licensed premises, sourced from the local authority or from business listings data (e.g. Yellow Pages)
- the increase in violent crime is due to an improvement in reporting to the police. Data that could be used to test this hypothesis include police recorded crime data, admissions to A & E departments for assault, and ambulance call-outs for violent offences. If police recorded crime data for violent offences had increased while the other two had not then this could be considered as a reason to explain the increase. Better still would be to use survey data to explore if public confidence in reporting violence offences has increased. This would however require surveys to be conducted both before and after any initiative that was put in place to help improve reporting.

In most circumstances more than one piece of information or dataset will be required.

The next stage involves establishing the legal basis for the sharing of this information: under what legal power can the information be shared? If the information relates to depersonalised information then there is no legal restriction on sharing data between CSP partners. If the information is personalised, then a clear legal basis must be established.

4.3.2 Step 2: Identify the source of this information

This step involves identifying the agency who can supply the information and the best person within that agency to contact. It is useful for a CSP to have a list of contacts to approach for information requests. If this has not been developed, then the Designated Liaison Officer for that agency should be consulted, along with the CSP Co-ordinator, to identify the contact point.

If a service has been contracted out to a provider and it involves the collection and management of data relevant to community safety, then it is important that any future data supply required from this privately managed service is provided free of charge. This condition should be written into the contract with the service provider.

4.3.4 Step 3: Explain why the information is required and how it will be used

Step 1 will have established the reasons why the information is required and can now be used to help justify the information request, backed up with the necessary legal basis if personal information is being shared. If the information request relates to depersonalised information then there is no legal basis for not sharing the information between CSP partner agencies.

4.3.4 Step 4: Extract the data and transfer the information

Step 4 involves the following tasks:

- identify the format in which the data are required e.g. paper or electronic format, as data records rather than a report of analysis results, in comma delimited format or some other common file format rather than in some unusual native database format;
- find out how long it will take for the information to be extracted and supplied; and
- agree with the information supplier the secure transfer process that will operate for the supply of data and ensure the required services are in place.

All transfers of information that relate to community safety should operate within a secure environment. The transfer of information involves removal to some other medium such as CD, USB memory stick or a file attached to an email. This requires the application of the standards as set out on the *Cross-Government Actions: Mandatory Minimum Measures* which defines the current arrangements for data transfer procedures (see http://www.cabinetoffice.gov.uk/csia.aspx). In summary, this requires:

- the information for transfer to the removable media to be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held;
- the removable media to be encrypted to a standard of at least FIPS 140-2 or equivalent, in addition to being protected by an authentication mechanism, such as a password;
- the transfer of data to removable media to be subject to monitoring by managers, the Designated Liaison Officer and the supplier of the information (i.e. the Information Asset Owner); and
- the individual responsible for the removable media to handle it themselves.

The use of a web-based transfer process is also permissible and encouraged where this offers a higher level of security. For an example, see Box 2, on p. 56.

4.3.5 Step 5: Consider whether any additional processing tasks are required

The data supplied may not always be of a standard that permits its immediate use. This may entail data being cleaned to correct for format errors, spelling and coding errors, and the correction of incomplete information where other sources can aid this correction.

If geographic coordinates are required to permit mapping in a geographical information system (GIS) and the data do not contain this information, but contain the address, a location or some other geographic reference (e.g. census output area code) then this information will also need to undergo additional processing. Some details of this process are described in Appendix 1A, but for more details on this consult your local GIS technician on how this can be performed. Most local authorities have a

GIS technician, usually located in the Planning Department, and all police forces have a person with some technical GIS skills who may also be able to provide some advice.

4.3.6 Step 6: Store the data securely

The information that has been supplied must then be stored securely. This requires the application of the standards as set out in the *Cross-Government Actions: Mandatory Minimum Measures* that define the current arrangements for data storage requirements (see http://www.cabinetoffice.gov.uk/csia.aspx). In summary, these require that:

- when information is held on paper, it must be locked away when not in use or the premises on which it is held must be secured;
- when information is held and accessed on ICT systems on secure premises, all agencies must apply the minimum protections for information as set out in the Suffolk Matrix shown in Figure 1. For more details on this matrix, see the *Cross-Government Actions: Mandatory Minimum Measures*.
- agencies should avoid use of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) for storage or access to such data where possible. Where this is not possible, all agencies should work to the following hierarchy:
  - The best option is to hold and access data on ICT systems on secure premises.
  - The second best option is to secure remote access, so that data can be viewed or amended without being permanently stored on a remote computer. This is possible over the internet using products meeting the FIPS 140-2 standard or equivalent. The National Technical Authority for Information Assurance, CESG, provides advice on suitable products and how to use them (www.cesg.gov.uk). See Box 2, on p. 56, which describes a solution such as this in Sunderland.
  - The next best option is to secure the transfer of information to a remote computer on a secure site on which it will be permanently stored. Both the data at rest and the link should be protected at least to the FIPS 140-2 standard or equivalent, using approved products as above. Protectively marked information such as data on serious violent crime offenders and sexual offenders, and individuals on witness protection, must not be stored on privately owned computers unless they are protected in this way.
  - In all cases, the remote computer should be password protected, configured so that its functionality is minimised to its intended business use only, and have up-to-date software patches and anti-virus software.

Figure 1. The Suffolk Matrix, used to define the standards for the minimum protection of government information. Source: Cabinet Office, 2009

Business Impact Level 'Protective Marking'	Types of data system included in category	e-GIF/CSIA		Network	External Access			
		Registration level	Authentication levels		Gov PC to WWW WiFi	WWW 'café' 3G data card	'PED' Bluetooth	Home Gov PC LAN Bootable USB
IL4 Confidential	Violent and sex offenders Witness protection	Level 3 Full ID verification with appropriate vetting and need to know measures	Physical/ personal/ procedural protection with appropriate technical authentication such as username + password or biometric/ certificate/token	x.GSi xCJX	Y[1]	N	N	Y[2]
					N	N	N	Y[3]
IL3 Restricted 'NHS Confidential'	Health record ContactPoint Crime record/ PNC	Level 2 Cross checked ID verification with appropriate vetting and need to know measures	Username + password/ Biometric digital certificate	N3 GSi CJX	Y	N	Y[4]	Y[5]
					Y[6]	Y[7]	N	Y[8]
IL2 Protect	General citizen data Finance systems	Level 1 Basic ID verification	Username + password and best commercial practice	GCSx Best commercial	Y	N	Y	Y
					Y	Y	Y[9]	Y
IL1/IL0	Google search BBC News	Anonymous	No authentication required	Any	Y	Y	Y	Y

Arrangements for material at higher protective markings are dealt with separately
1 Via 'thin client internet browse-down'
2 Via hard-aired Government issue secure laptop
3 Requires a strong business case and CESG advice
4 Via CESG approved product such as Blackberry, Ref. CESG Procedures for Blackberry Administrators and CESG Security Procedures for Blackberry users
5 Via CESG-approved VPN or validated Manual T or Manual V solutions
6 Implementations must be compliant with CESG Manual Y
7 Via Government issue secure laptop with software encryption
8 Using software-based cryptography
9 Requires a strong business case and CESG advice

Box 2. Sunderland CSP CyberArk Vault

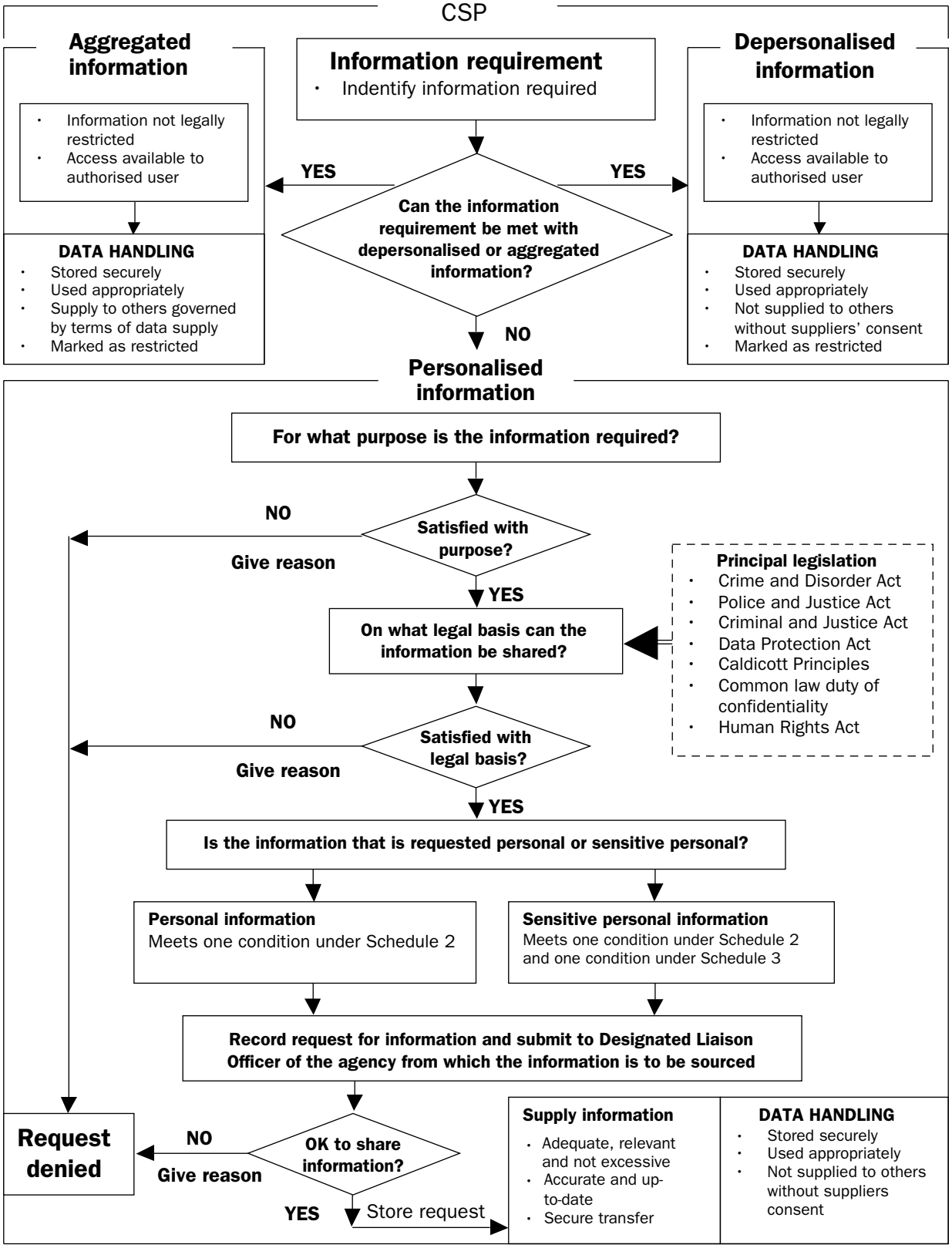
The Sunderland CSP operate a 'Vault' procured from CyberArk to facilitate the secure transfer and storage of community safety information.

The Vault provides a single online electronic mechanism for the transfer, storage and extraction of information by CSP partner agencies, using technology of military security standard. Login access to the Vault (which requires a user ID and password administered by an officer in the CSP) is only granted to those that have been authorised by the CSP Co-ordinator. This login then fits against a profile that defines what data the person can and cannot have access to.

Data transfers to the Vault are performed using a process that automatically encrypts the information as it passes through cyberspace. When a user accesses the Vault and extracts information, the transfer of information to their desktop is also automatically encrypted. The user can decide to work on the version with this link to the Vault still established. This means that after the data has been viewed the Vault will extract the information that was transferred to the user's desktop and place it back in the Vault, meaning that no traces of the data are left on the user's computer. The user can if they wish make a copy of the data that was transferred but are then subject themselves to the standard handling conditions that are required for government data.

The use of The Vault also means that data is held in one place for many users to extract, and therefore helps minimise database handling tasks. For example, each month when crime data is supplied in to the Vault it only requires an administrator to append this monthly update file to the existing archive of crime data. This data update can then be accessed along with other archived data by users with authorised access.

Figure 2. Flow model summarising the processes involved in sharing information for community safety purposes (performance monitoring, intelligence development or service delivery)



4.4 IMPLEMENTING AN INFORMATION-SHARING FRAMEWORK

Many CSPs that have matured their information-sharing processes have now developed them into a framework process model that supports the continual efficient and effective exchange and use of information. This type of framework can now be seen to operate across the CSPs in Greater Manchester, Cornwall, Cheshire and across the 12 CSPs in the North East of England.

An information-sharing framework has the following benefits in promoting information sharing.

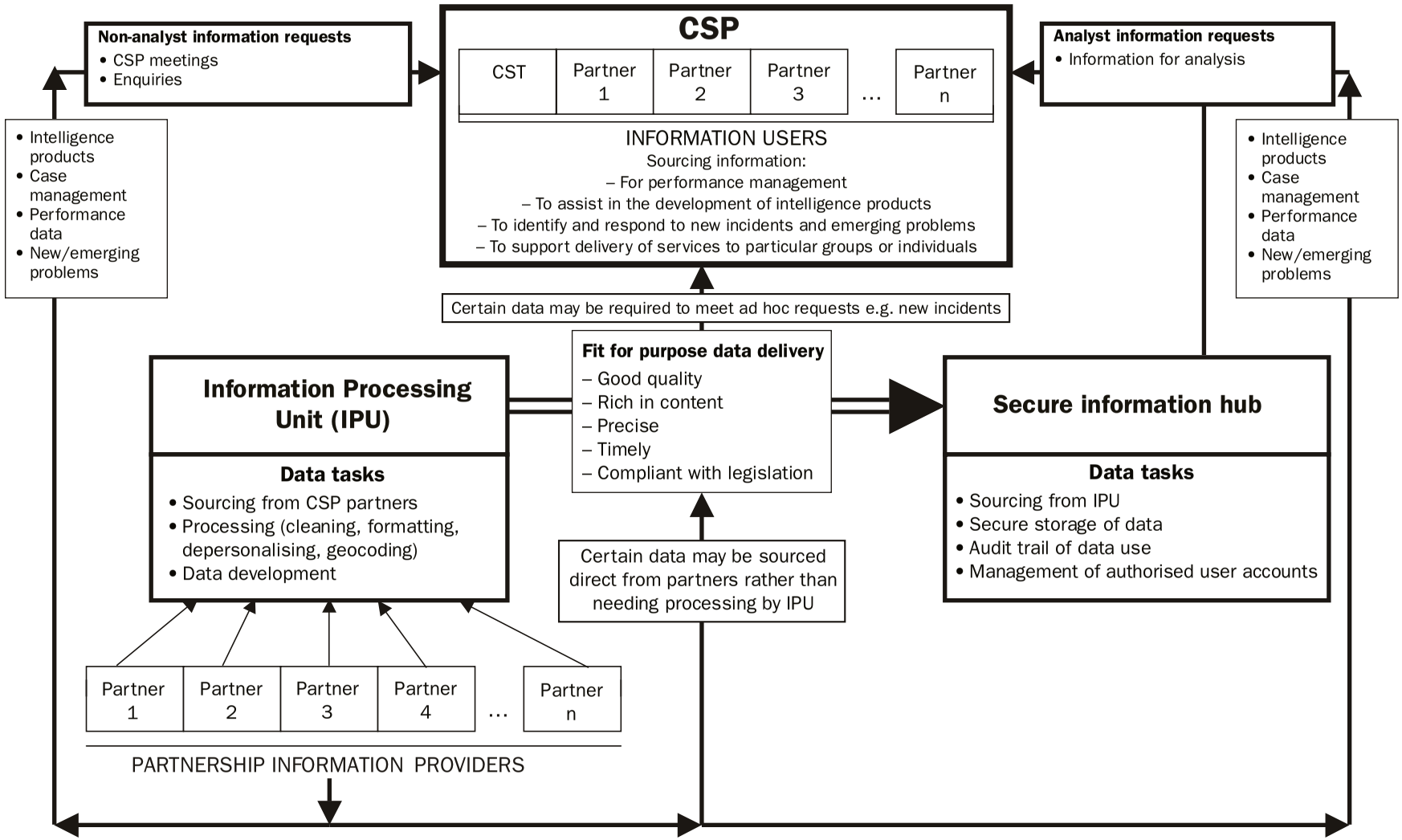
- CSPs explore and make use of more efficient processes to facilitate information sharing such as improving the services and arrangements for sourcing data, data cleaning and data storage, often resulting in the first instance in the establishing of an information hub (also known as a data warehouse) that acts as the central storage facility for CSP information that is shared. Many CSPs have also taken the decision to contract out the sourcing, cleaning, geocoding and supply processes, in most cases to their local public observatories. See Box 3 for an example.
- A defined structure for information sharing helps the CSP, particularly in an area where the framework is regional, to benefit from a more co-ordinated programme of information sharing that works to collectively improve the range, quality and content of data they can use for their intelligence-led business processes.
- A defined structure for information sharing helps the CSP to reflect on and identify ways in which technological improvements can be made to help to widen the access to information stored in a centralised warehouse.
- A single information-sharing framework helps to promote the key principles involved in information sharing more effectively. This includes ensuring that partner agencies are aware of the need for a problem-oriented approach to information sharing, focusing on the sharing of core information over peripheral information.

Figure 3 shows a process model for this type of information sharing framework. The process model is driven by meeting the information requirements of the CSP (readers should start at the CSP box when interpreting this model). Data sourced from partner agencies and processed is specified by the CSP, with a service facility being in place to perform the necessary data exchange tasks. In some CSPs this is a function that has been contracted out (see Box 3) or performed by an officer or a dedicated team in the CSP.

Information is delivered to an information hub in a manner that ensures the data are fit for purpose. The information hub then acts as a secure data storage facility that authorised users can access to extract data for supporting partnership intelligence development. To enable access to the information by a wide range of authorised users most typically requires this hub to be a web-based data storage tool, implemented with the necessary security conditions (see Section 4.2.6).

Certain data required for analysis may not require any data cleaning or geocoding, so these data can be channelled into the hub direct from their source. CSPs often also benefit when they can access recording systems in real time for the purpose of investigating specific enquiries. This is also illustrated in the framework by the direct link between users and the partner agency information providers.

Figure 3. Process model for information-sharing to support the information requirements of CSPs



Box 3. Contracting out information sharing processes in Greater Manchester and the North East of England

Across Greater Manchester, the ten borough CSPs make use of the Association of Greater Manchester Authorities to arrange the sourcing, processing and supply of community safety information. Similarly, across the North East of England, the 12 CSPs in this region have Service Level Agreements with their respective sub-regional observatories to facilitate similar processes. As a result of these processes, CSP analysts are no longer burdened with the task of negotiating and facilitating the supply of information from partner agencies, which in some areas is known to take up at least a third of their time. Instead, analysts can focus more time on analysis in the knowledge that data can be more easily accessed when it is required, with a stamp indicating with some assurance its level of quality. Across a region, the application of a single information-sharing framework also helps to ensure that there is consistency in the information that can be sourced: information that is fit for purpose in one area is available to the same standard in another area, and cannot be jeopardised by the agency in that area not providing the necessary information.