Safer Stockton Partnership

Information Sharing Protocol 2016

Safer Stockton Information Sharing Protocol

The purpose of sharing information within the Safer Stockton Partnership is to:

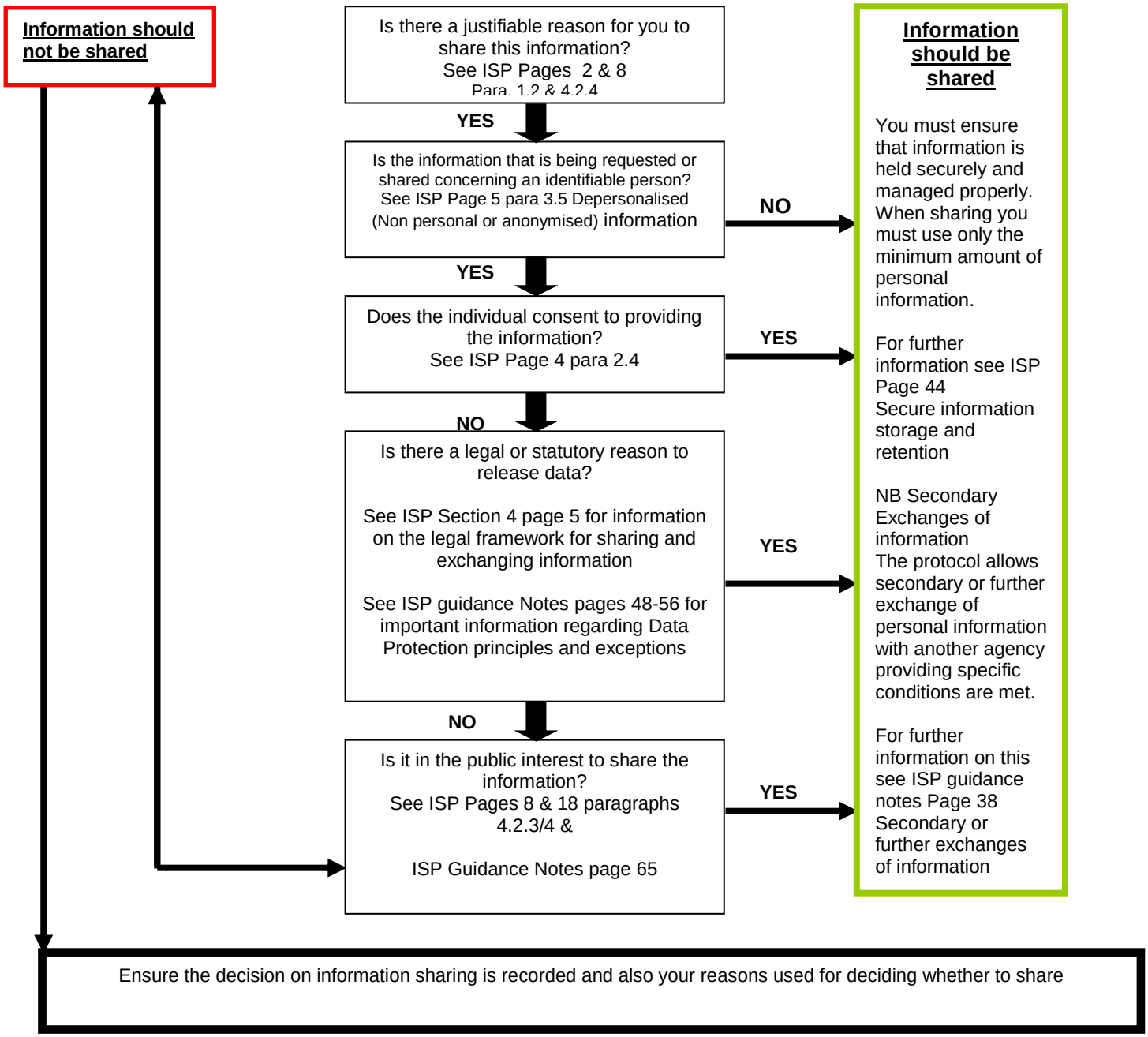
a) Prevent crime and disorder, anti-social behaviour and substance misuse and,
b) Apprehend and prosecute offenders.

If you are asked or wish to share information you should consider the following. Each option is equally valid to enable information disclosure and only one condition needs to be satisfied:

- Has the data subject provided consent?
- Is the agency legally empowered to share the information and are the conditions of Schedules 2 and 3 of the DPA satisfied?
- Is there an over-riding public interest for disclosure (see page 65 of the Guidance Notes)
- Is there an exemption under the Data Protection Act? These can be used on a case-by-case basis and include exemptions for the apprehension and prosecution of offenders (Section 29) and prospective legal proceedings (Section 35). For more information please see pages 15&16 of the Guidance Notes.

Any disclosure or sharing of personal information must have regard to both common and statute law. For example defamation, the common law duty of confidence (see page 19 of the Guidance Notes). and the data protection principles. All disclosures must be:

a) On a case by case basis.
b) Proportionate
c) With a minimum amount of information necessary to achieve the purpose.
d) Only with those individuals who have a right to access the information.



Contents

List of Appendices

Acknowledgements

This Information Sharing Protocol has been adapted from the Hartlepool, Nottinghamshire, Surrey and Middlesbrough Information Sharing Protocols.

1. Background and purpose of the protocol

This document should help with decision making and help direct appropriate responses to prevent and reduce crime, anti-social behaviour (ASB) and to: apprehend and prosecute offenders, to reduce re-offending, to increase public reassurance and reduce the fear of crime for residents within the Borough of Stockton-on-Tees.

This Information Sharing Protocol (ISP) is owned by the Safer Stockton Partnership (SSP). Any enquiries about the content of the document should be directed to Steven Hume, SBC Community Safety Team, Stockton Police Station, The Square, Stockton-on-Tees, TS18 1TZ.

1.1 Background

This protocol is complemented by the Safer Stockton Partnership Community Safety Information Sharing Guidelines which provide a strategic set of principles to be followed when sharing and/or jointly processing personal information. The Information Commissioners Office enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. This protocol conforms to the ICO guidance.

This ISP should be used in conjunction with the ISP Guidance, which sets out the procedures for information exchange in greater detail found at Appendix 1.

1.2 Purpose

The purposes of sharing information[1] within the Safer Stockton Partnership (SSP) are to direct the appropriate response to the following for residents within the Borough of Stockton-on-Tees.:

a) Preventing crime and anti-social behaviour
b) Reducing crime, anti-social behaviour and the fear of
c) Apprehending and prosecuting offenders
d) Reducing re-offending
e) Increase public reassurance and reduce the fear of crime / asb

This ISP seeks to:

a) Support effective performance monitoring
b) To develop intelligence in the form of Strategic Assessments, Problem Profiles, and other associated tactical documents Facilitate the secure exchange of depersonalised and personalised information between signatory agencies
c) Govern the use and management of information by the SSP for the purposes of developing and implementing partnership plans and tactics for crime and disorder reduction including anti-social and other behaviour adversely affecting the community/ environment, tackling substance misuse and adult and youth offending, including the use of restorative approaches.
d) Support the actions and delivery of plans of the SSP multi-agency area located JAG Meetings and problem solving groups involved in tackling crime, anti-social behaviour and substance misuse, including the Right to Review (Community Trigger) introduced by the Anti-social Behaviour Crime and Policing Act 2014.

[1] For the purposes of this protocol the term “information” will be used to include “data”, as defined in the Data Protection Act 1998 and “information “ as defined in the Crime and Disorder Act 1998 and ASB Crime and Policing Act 2014.

e) Assist the work of Public Health to raise awareness and tackle and substance misuse, domestic abuse and any other associated health risk associated with crime within the Borough.
f) Assist the work of the Youth Offending Service in developing and delivering the Youth Justice Plan and working in partnership with other agencies in delivering the Youth Inclusion Programme and Youth Inclusion and Support Panels.
g) Assist the work of the Local Criminal Justice Boards
h) Support the development of and continuation of secure information exchange in response to Integrated Offender Management (IOM) and Prolific and Priority Offender schemes / work to reduce repeat offending.
i) Enable the exchange of personal information between agencies dealing with cases of domestic abuse and violence
j) Support information exchange for the purposes of fire safety and arson reduction within communities
k) Enable statutory authorities to more effectively meet their obligations under Section 17 of the Crime and Disorder Act 1998 and the amendments made by the Police and Justice Act 2006 and the ASB Crime and Policing Act 2014.
l) Ensure that the exchange of information, including by electronic means, is undertaken securely and safely.
m) Provide guidance on the storage, retrieval and disposal of information.
n) Ensure clear processes to aide response to Freedom of Information requests, particularly for those where more than one agency is contacted for information that relates to another originating agency.

This ISP may not supersede existing information sharing protocols, although partner agencies have agreed to operate under this ISP wherever possible. Information exchange for Multi-Agency Public Protection Arrangements (MAPPA) and Safeguarding are excluded from this protocol.

Agencies should ensure that they have effective data protection processes in place for responding effectively and safely to other requests for personal information that may be made by agencies in pursuit of their main business outside the areas covered by this protocol. Although the principles on which this ISP is based will still apply, appropriate internal procedures should also be in place.

2. Sharing Information

2.1 What is information sharing?

Information sharing involves a physical exchange of information between one or more individuals or agencies. Data exchange seeks the same end, but relates more specifically to information recorded in a form that can be processed by equipment automatically, (usually electronically), in response to specific instructions.

2.2 Why share information?

> *"Information sharing is the cornerstone of delivering shared understanding of 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)

Sharing information is fundamental to the success of any partnership plan to reduce crime and disorder, to promote community safety and tackle substance misuse. The use of good quality information and intelligence is essential in identifying and limiting the activities of those committing crime and disorder and in tackling those problems that adversely affect community safety and quality of life, including anti-social and other behaviour adversely effecting the environment. It can also help to develop effective interventions at a much earlier stage to prevent those identified as being at risk from becoming offenders or victims.

The more complete the picture of an individual's circumstances – not just contact with police or other community safety agencies, but also knowledge of support already provided by agencies or social issues, family or life stresses – the more informed and effective any intervention agreed and delivered will be.

2.3 Benefits of information sharing

The benefits of sharing information are:

a) Better informed decision making and joined up working.
b) Improved inter-agency relationships.
c) Better profiling of crime and disorder activity to enable the more effective targeting of resources.
d) A more joined up approach to providing protection to the public.
e) Regular monitoring and evaluation of community safety initiatives.
f) Reduction in crime and disorder, and the fear of.

2.4 Consent

Many of the data protection issues surrounding sharing personal information can be satisfied if the data subject (i.e. the person to whom the information relates) gives you explicit, informed consent to share the information specified with others in writing. This means that a data subject must be aware of and understand the purposes for which their data are being processed. When working with an individual it is good practice to obtain consent before sharing personal information. The Data Protection Act makes provision for the fact that gaining consent is not always suitable particularly where this could lead to prejudicing any activity around preventing or detecting an offence. ISP form 1 (Appendix 4) is a consent form suitable for both the data subject and any identifiable third party. This form, or an organisations own personal version of the form, should be used when obtaining consent to disclose personal information. Forms can be used to secure consent from either the subject of the information, or from anyone else who may be identified or identifiable as a result (e.g. a witness, family member etc)

Careful consideration should be given before sharing the details of victims, witnesses or people who have made a complaint, unless you have obtained their permission in writing. Information about victims, witnesses or people who have made a complaint must always be kept separately. This will apply even if they are not named but can be identified by inference. It is recommended that all agencies apply a policy of removing third party data when sharing information.

3. Definitions

Crime
Defined as any act, default, or conduct prejudicial to the community the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty[2].

Anti-social behaviour
Means acting in a manner which causes or is likely to cause harassment, alarm, or distress to one or more persons who are not of the same household.

Anti-Social Behaviour
Refers to the level or pattern of anti-social behaviour within a particular area.

Incident
An incident report is any communication, by whatever means, about a matter that comes to the attention of the police. All reports of incidents, whether from victims, witnesses or third parties, and whether crime-related or not, result in the registration of an incident report by the police. An incident is recorded as a crime if, on the balance of probability, the circumstances as reported amount to a crime defined by law and there is no credible evidence to the contrary.

Depersonalised (Non personal or anonymised) information
Depersonalised information is defined as information where any reference to or means of identifying a living individual has been removed. This is any information, which does not (or cannot be used to) establish the identity of a living individual. There are no legal restrictions on the exchange of depersonalised information.

Information in the public domain
This type of information incorporates any information, which is publicly available, whether it relates to an individual or not.

Personal information
Personal information means information, which relates to a living individual who can be identified either directly from the information or from the information and any other information which is in the possession of or is likely to come into the possession of the data controller (see Guidance Notes page 12).

Sensitive personal information (defined under the Data Protection Act 1998)
Defined as information describing:

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

[2] The term penalty refers to any punishment fixed by law.

Although not defined under the Data Protection Act 1998 as sensitive personal information, for the specific purposes of this protocol the following categories should be processed as sensitive, personal information:

a) information relating to victims
b) information relating to witnesses

4. The legal framework for sharing and exchanging information

4.1 Sharing Information

4.1.1 The power to disclose or share information

You must process personal information in line with the law, for example by taking account of defamation, the common law duty of confidence and the data protection principles, unless any exemptions under the Data Protection Act apply.

4.1.2 Crime and Disorder Act (1998)

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

4.1.3 Criminal Justice and Court Services Act (2000)

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

4.1.4 Police and Justice Act (2006)

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

The Police and Justice Act 2006 also places a statutory duty on the strategy group of all crime and disorder reduction partnerships to prepare an information sharing protocol[3]. The protocol must cover the sharing of information under the new duty to share specified depersonalised datasets and also any additional information sharing between the

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

responsible authorities and other agencies named under Section 115 of the Crime and Disorder Act 1998, including personal information. A statutory duty has also been placed on each responsible authority to nominate a designated liaison officer whose role is to facilitate the sharing of information with other partners.

4.1.5 ASB Crime and Policing Act 2014

The Anti-Social Behaviour, Crime and Policing Act 2014 Community Trigger process requires the relevant bodies to share relevant information for the purpose of carrying out a case review. The relevant bodies may request any person to disclose information for the purpose if a Community Trigger review. If the request is made to a person who exercises public functions and they possess information they must disclose it. The only exception to that is where to share the information would be either:

- in contravention of any of the provisions of the Data Protection Act 1998; prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000

Other than these two exceptions, disclosure of information for the Community Trigger does not breech any obligation of confidence or any other restriction on disclosure of information.

4.1.6 Other relevant Acts

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

- Children Act 1989
- Children Act 2004
- Domestic Violence Crime and Victims Act 2004
- Anti-Social Behaviour Act 2003
- Sexual Offences Act 2003
- Local Authority and Social Services Act 1970 (amended 2003)
- Housing Act 1996
- Housing Act 2004
- Police and Criminal Evidence Act 2001
- Anti-Social Behaviour Crime and Policing Act 2014
- Offender Rehabilitation Act 2014
- Counter-Terrorism and Security Act 2015

4.2 Legislation governing the sharing of information

4.2.1 Data Protection Act (1998)

The Data Protection Act (DPA) sets out principles which govern the way information is processed and should not be seen as prohibitive of the relevant sharing of personal information.

The DPA contains a number of exemptions which enable the sharing of information for the purposes of Prevention, Detection of crime and the apprehension, prosecution of offenders (Section 29.

The DPA also requires that information must be accurate, relevant, kept up to date, held no longer than necessary, and be kept and exchanged securely. The DPA also gives individuals or ‘data subjects’ certain rights with regard to their personal information.

An organisation which processes information relating to identifiable living persons is legally obliged under the Data Protection Act to make a notification with the Office of the Information Commissioner, the government office responsible for the operation and enforcement of the Data Protection Act and the Freedom of Information Act. **Each agency must ensure that they hold a current notification with the Information Commissioner[4] to share appropriate information under this protocol.**

Schedule 1 of the Data Protection Act includes eight principles in relation to the processing of personal information:

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

For more information, including details of the Schedules, please see pages 55-59 of the Guidance Notes.

4.2.2 Human Rights Act (1998)

This Act should be taken into account in establishing whether the purpose of information exchange is lawful.

The Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be compatible with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may

[4] An independent official appointed by the Crown to oversee the Data Protection and Freedom of Information Acts – see their website at www.informationcommissioner.gov.uk
[5] Even in the event that the Section 29 (prevention and detection of crime) Data Protection Act exemption is relied upon, Schedules 2 and 3 conditions must still be satisfied.

be subject to a legal action under section 7 of the Act. This obligation should not be seen solely in terms of an obligation not to violate Convention Rights but also as a positive obligation to uphold these rights.

Article 8 of the Act is of particular relevance to information sharing as this relates to 'the right to respect for private and family life'.

4.2.3 Common law duty of confidentiality

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

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

Common Law judgements have identified a number of exceptions:

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

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

4.2.4 The Caldicott Principles

The Caldicott Principles are guidelines that are followed by Social Care and Health professionals regarding the use of person-identifiable and confidential information. Established following the 1997 Caldicott Committee Report, and reviewed again in 2013, there are six general principles for the safe handling of personal- identifiable information, that provide the guidelines to which the NHS works. They work hand-in-hand with the Principles of the Data Protection Act 1998. The principles are:

1. Justify the purpose
2. Don't use personally identifying information unless it's absolutely necessary.
3. Use the minimum amount necessary of personally identifying information
4. Access to personal information should be on a strict need to know basis
5. Everyone should be aware of their responsibilities with regard to personal information. Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect an individual's confidentiality.
6. Understand and comply with the law

Each health and social care organisation has a Caldicott Guardian responsible for:

a) Agreeing and reviewing information sharing policy
b) Ensuring the organisation satisfies the highest practical confidentiality standards
c) Acting as the conscience of the organisation
d) Advising on lawful and ethical processing of information
e) Resolving local issues

f) Ensuring a record of resolved issues is kept

4.2.5 Freedom of Information Act (2000)

Any person under the provisions of the Freedom of Information (FOI) Act may request information held by public sector authorities. Under certain circumstances an authority may refuse to supply information because they believe that one or more of 24 possible exemptions may apply to the information being requested. For example, disclosure may breach other legislation such as the Data Protection Act or the information may already be widely available in the public domain. Unless these exemptions apply, public authorities are obliged to provide the information within 20 working days of the receipt of a request.

Since the Data Protection Act continues to govern access to personalised information, it is mainly non-personal information that is affected by the provisions of the FOI. This will include information in any form, including informal, electronic and database records. The FOIA is a complex piece of legislation. Almost all authorities have trained specific staff to deal with applications for information made under the Act. Their advice should be sought in the event of any questions arising about the Act, which are not answered within the ISP Guidance Notes.

A request may be received by an authority for any information that it holds, not just that which it has generated itself or relates to its own activity. Should a request under FOI be received by one authority for information which originated with another authority, it is a requirement of this ISP that the originating authority is consulted before any release is made.

4.2.6 Local Government Act (2000)

<u>Promotion of Well-being</u>

This Act gives every local authority the power to do anything which they consider is likely to achieve any one or more of the following objects:

1. a) the promotion or improvement of the economic well-being of their area,
   b) the promotion or improvement of the social well-being of their area, and
   c) the promotion or improvement of the environmental well-being of their area.

2. The power under subsection (1) may be exercised in relation to or for the benefit of:

   a) the whole or any part of the local authority's area, or
   b) all or any persons resident or present in a local authority's area.

3. In determining whether or how to exercise the power under subsection (1), a local authority must have regard to their strategy under Section 4.
4. The power under subsection (1) includes power for a local authority to:

   a) incur expenditure
   b) give financial assistance to any person
   c) enter into arrangements or agreements with any person,
   d) co-operate with, or facilitate or co-ordinate the activities of, any person.
   e) Exercise on behalf of any person any functions of that person, and
   f) Provide staff, goods, services or accommodation to any person.

5. The power under subsection (1) includes power for a local authority to do anything in relation to, or for the benefit of, any person or area situated outside their area if they consider that it is likely to achieve any one or more of the objects in that subsection.

6. Nothing in subsection (4) or (5) affects the generality of the power under subsection (1).

Limits on power to promote wellbeing

1) The power under section 2(1) does not enable a local authority to do anything which they are unable to do by virtue of any prohibition, restriction or limitation on their powers which is contained in any enactment (whenever passed or made).

2) The power under section 2(1) does not enable a local authority to raise money (whether by precepts, borrowing or otherwise).

3) The Secretary of State may by order make provision preventing local authorities from doing, by virtue of section 2(1), anything which is specified, or is of a description specified, in the order.

4) Before issuing any guidance under this section, the Secretary of State must consult such representatives of local government and such other persons (if any) as he considers appropriate.

5. Agencies involved in information sharing (Section 5 of Crime and Disorder Act)

5.1 Responsible Authorities

Responsible authorities are under a statutory duty to ensure that key agencies come together to work in partnership. Section 5(1) of the Crime and Disorder Act identifies these Responsible Authorities with further regulation being provided by the Police Reform Act 2002 and the Police and Justice Act. For the purposes of this ISP the following organisations are considered as Responsible Authorities:

a) Stockton Borough Council
b) Cleveland Police (Chief Police Officer).
c) Cleveland Fire Brigade (as amended under the Police Reform Act 2002)
d) Clinical Commissioning Group (as amended under the Health and Social Care Act 2012)
e) Community Rehabilitation Company Limited – Probation (as amended under the Offender Rehabilitation Act 2014)

While the term 'partnership' is applied to all those who sit round the table, legally, the responsible authorities are the only bodies or agencies under the duty to meet the regulatory requirements.

5.2 Who can be asked to co-operate?

Co-operating bodies refer to agencies that are important in supporting the development of strategic assessments and the implementation of partnership plans. Section 5(2)(c) of the Crime and Disorder Act provides details of persons or bodies required to co-operate with the Responsible Authorities in their exercise of the functions conferred by section 6 of that Act.

From 15th November 2012 the Office of the Police and Crime Commissioner are now considered as a co-operating body.

Responsible Authorities are required to work in co-operation with, parish councils, NHS Trusts, NHS Foundation Trusts, proprietors of independent schools and governing bodies of an institution within the further education sector and to work closely with Drug (and Alcohol) Action Teams in two tier local authority areas.

From 31 July 2007, Registered Social Landlords (in England) were made co-operating bodies with the responsible authorities of community safety partnerships. The Housing Act 2004 also amended Section 115 of the Crime and Disorder Act 1998 allowing the disclosure of information to Registered Social Landlords for the purposes associated with Section 1 of the Crime and Disorder Act which is in relation to anti-social behaviour.

Responsible Authorities are also expected to invite a range of local private, voluntary, other public and community groups including the public to become involved partnership activity. Invitees asked to participate are drawn from agencies whose knowledge will assist CDRP members to reduce crime and anti-social behaviour more effectively.

Section 5(3) of the Crime and Disorder Act provides descriptions of persons or bodies, at least one of which must be invited by the Responsible Authorities to participate in the exercise of the functions conferred by section 6 of that Act (primarily the development and delivery of a partnership strategy for the reduction of crime and disorder and tackling drug abuse).

5.3 Relevant Authorities for the purposes of Section 115

The effect of Section 115 of the Crime and Disorder Act 1998 is to allow disclosure to a "relevant authority". Relevant authorities are defined as:

a) Police forces
b) Local authorities (such as district, borough & county councils)
c) Community Rehabilitation Company Limited - Probation (as amended under the Offender Rehabilitation Act 2014)
d) Fire and rescue authorities
e) Health Authorities – Clinical Commissioning Group(as amended under Health and Social Care Act 2012), Strategic Health Authority, NHS Trust, and NHS Foundation Trusts.
e) A person registered under Section 1 of the Housing Act 1996 as a social landlord (by virtue of Section 219 of the Housing Act 2004)

5.4 Level A and Level B Partners

This ISP designates two levels of agency determined by the extent of their involvement with CDRP and criminal justice activity.

In most cases the exchange of personal information is likely to take place between Level A partners and it is strongly recommended that electronic exchange is restricted to this group (see 8.2). Level A partners are:

Data Controller	ICO Registration	Expiry Date
Cleveland Police		
Stockton Borough Council		
Cleveland Fire Brigade		
North East Strategic Health Authority		
North Tees & Hartlepool NHS Foundation Trust		
Stockton Youth Offending Service		
Community Rehabilitation Company Limited - Probation		
Crown Prosecution Service		
Ministry of Justice (HM Courts & NOMS)		
Victim Support		
Thirteen Group		
Lifeline Project Limited		
Clinical Commissioning Group		
Harbour Support Service		
Lifeline		
Department of Work & Pensions		
Catalyst		

Registered Social Landlords are also designated as cooperating bodies. Where housing authorities are seeking injunctions to prevent nuisance and annoyance separate protocols established between each RSL and the Police should govern the process for information exchange.

When services are being commissioned it is recommended that all service level agreements set out the requirement for information sharing and being a signatory to the ISP.

Increasingly voluntary sector agencies are providing key support services essential for the functioning of CSPs and DAATs. It is strongly suggested that services commissioned to provide support for drug and alcohol treatment and sexual assaults and domestic abuse are signatories to the protocol as Level A partners. When services are being commissioned it is recommended that all service level agreements set out the requirement for information sharing and being a signatory to the ISP.

Any other agency wishing to become a Level A partner can only do so with consent from all of the responsible authorities which are signatories to this protocol.

Level B partners are designated as any other agencies that are signatories to this Protocol. Most Level B partners are less likely to take a central role with the processes for sharing personalised information but may use the protocol for sharing depersonalised information.

All other partners will be allowed to attend relevant multi-agency groups on an invitee basis and be invited to attend the groups as and when required by the relevant chair. Invitees will not be involved in any information exchange whatsoever and will only attend groups for information purposes.

5.5 Responsibilities of signatories

It is the responsibility of signatories to ensure that:

a) They are correctly registered with the Information Commissioner for processing personal data.
b) The data protection principles are upheld
c) The information shared is kept secure and confidential
d) Information is accurate and up to date
e) Realistic expectations prevail from the outset
f) Professional ethical standards are maintained
g) A mechanism exists by which the flow of information can be controlled
h) Appropriate staff training is provided on this protocol
i) Adequate arrangements exist to test adherence to the protocol
j) Records are maintained of decisions to share or withhold information
k) All instances of non-compliance and any breaches of the ISP are addressed.

The Information Sharing Agreement should be signed by the Chief Officer for that organisation as defined by the Data Protection Act. All signatories must ensure that the protocol is fully implemented within their organisation and should develop procedures to ensure that all staff are aware of the issues around information sharing, and all Designated Officers (see 6.4 for explanation of this role) are conversant with the ISP and their responsibilities.

More information on meeting the responsibilities of this ISP are contained in the Guidance Notes.

5.6 Information exchange outside the area

There will be occasions when agencies may need to make (or may receive), requests for personal information from agencies operating outside the area covered by the protocol. With due regard to the Data Protection Act restriction confining information exchange to the European Economic Area, the principles of this protocol continue to apply and exchange should take place between appropriate Responsible Authorities in the two areas.

5.7 Involvement of external agencies in the protocol

This protocol does not cover every exchange of information. Release of information for analysis and evaluation by external researchers, (by universities or consultants),

or subcontractors requires a formal written agreement. Careful consideration should always be given to the necessity of sharing personal information. Responsibility for ensuring compliance and security rests with the agency that subcontracts the work. They must ensure that the subcontractor is obliged to fully comply with the relevant legislation as outlined in Section 4 of this Protocol.

6. Information Disclosure and Exchange

6.1 General principles

Disclosure is considered to be a form of information processing under the Data Protection Act. As a result personal information needs to be processed fairly and lawfully, and should not be processed unless at least one condition from Schedule 2 and for sensitive information one condition from Schedule 2 and 3 is met, (for more information please see page 17 of the Guidance Notes).

The Data Protection Act is designed to protect the rights of the data subject so that where organisations hold information about an individual they are legally obliged to ensure they use the information appropriately and retain it securely. There are certain circumstances where it is considered appropriate to disclose personal information to other agencies. Each of the options listed below (a-d) are equally valid to enable information disclosure and only one condition needs to be satisfied. These are:

a) Where the data subject has provided consent
b) Where an agency is legally empowered to do so and the conditions of Schedules 2 and 3 of the DPA are satisfied
c) Where there is an overriding public interest for disclosure (see pg16 and 64 of Guidance Notes)
d) Where there is an exemption under the Data Protection Act. These can be used on a case-by-case basis and include exemptions for the apprehension or prosecution of offenders (Section 29) and prospective legal proceedings (Section 35). For more information please see pages 15 and 53-55 of the Guidance Notes.

Any disclosure or sharing of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidence (see page 64-65 of the Guidance Notes), and the data protection principles.

All disclosures must be:

a) On a case by case basis
b) Proportionate
c) With a minimum amount of information necessary to achieve the purpose
d) Only with those individuals who have a right to access the information.

Extreme care and careful consideration should be taken where the disclosure of information includes details of witnesses, victims or complainants and, wherever possible, consent from any identifiable third party should be sought (ISP Form 1, page 27 of the Guidance). It is recommended that legal advice is taken where the disclosure of information would include any third party information.

If information is disclosed the requesting organisation must store the information securely and destroy when no longer required.

The underlying principle of the protocol is that an agency will always retain ownership of the personal information it discloses to another member of the partnership. The identity of the originator must therefore be recorded against the relevant information. A recipient of such information must obtain the consent of the original data owner before making a further disclosure.

Information shared under this protocol should be shared through the following mechanisms:

- Designated Officers
- Multi-agency/problem-solving groups.

The considerations around disclosure and exchange of information apply equally to paper and electronic records. All considerations and procedures around the secure exchange and principles of evaluation of requests and retention of information in this ISP apply to all exchanges, irrespective of medium.

6.2 Requesting and exchanging information

The Guidance Notes include forms that could be used for requesting information or permissions. These forms can be used for all mediums for the request and exchange of information, including electronic.

a) ISP1 – Consent to disclose personal information
This form can be used to secure consent from either the subject of the information, or from anyone else who may be identified or identifiable as a result (e.g. a witness, family member etc)
b) ISP2a – Request for personal information on an individual subject.
This form can be used by a Designated Officer to request personal information from another Designated Officer and must give comprehensive reasons as to why the purpose is legitimate
c) ISP2b – Record of multi-agency/problem-solving group meetings.
This form may be used to record information sharing at multi-agency/problem-solving group meetings.
d) ISP3 – Request for non-personal information.
This form can be used when non-personal information is needed.
e) ISP4 – Altering information (i.e. correcting inaccuracies or updating information).
This form can be used when information needs to be corrected or updated.
f) ISP5 – Mandate for an exemption to subject access rights (i.e. under Data Protection Act). This form can be used by the organisation's registered Data Protection Officer to provide the necessary mandate for an exemption under Section 31 of the Data Protection Act. This will endorse a decision to withhold personal information from the subject.

All requests for information should be responded to in a timely manner.

6.3 Exceptional and emergency exchange

There will occasionally be circumstances in which information is required urgently and the form based exchange process cannot be followed. In these circumstances, the phone procedure detailed on page 42 of the Guidance Notes should be followed. Any exchange made under this provision MUST be backed up by paper exchange using the ISP forms no later than five days after the original exchange took place.

6.4 Designated Officers

The signatories to this protocol will nominate as many Designated Officers to process or initiate requests for any personal information. Agencies should empower their representatives on multi-agency/problem-solving groups to share information by appointing them as Designated Officers.

Any person requiring information from another agency should submit the request through their agency's Designated Officer. The exchange of information may be recorded using the approved forms on pages 27-34 of the Guidance Notes. All information exchange should be kept in such a way that they can be subject to audit.

The Guidance Notes include a checklist for Designated Officers (pages 20-21) which will help them to assess if a request for personal information is appropriate and justified. Essentially, this requires the Designated Officer to consider, when asked to share information in response to a request:

- Whether they have a legal power to share the information
- Whether to do so will be adhering to the law (both common and statute law)
- Whether it would be in the public's interest to share the information
- Whether there is a clear justification and purpose for needing the information requested.

A list of Designated Officers will be made available and updated on a regular basis by the local Community Safety Team.

6.5 Designated Managers

The signatories to this protocol will nominate one individual from their organisation to be responsible for the management of their Designated Officers list. Their primary role will be to maintain the list/register of Designated Officers and to inform business managers responsible for nominating Designated Officers of the requirement to replace any Designated Officer who ceases to be involved in that role.

Under the Police and Justice Act 2006 Responsible Authorities have a statutory duty to nominate a Designated Liaison Officer whose role is to proactively facilitate information sharing with other partners.

6.6 Multi-agency/problem solving groups

Multi agency/problem solving groups consist of relevant agencies brought together to address community safety issues. As well as using depersonalised information to analyse current trends and hotspot locations, these groups discuss and agree action to reduce the negative effect that problem individuals and families associated with antisocial behaviour or criminality have on the wider community. Examples of issues dealt with include persistent criminal or anti social behaviour, race/hate crime, misuse of alcohol or drugs and vulnerable people e.g. street drinkers or the homeless.

This protocol recommends these multi-agency/problem solving groups as the most appropriate forum in which to exchange personal information. Decisions on disclosures reached at meetings must be minuted. The guidance notes (pages 22-24) provide more detail on information sharing at these meetings.

6.7 Depersonalised information sharing

Data hubs in each area provide officers of partner agencies with access to geographical profiling information on crime and disorder, fire, offending and other information relevant to community safety issues. These data hubs have established protocols and information sharing arrangements with each of the agencies supplying information. The disclosure of depersonalised information is not legally restricted, however, it is recommended that where depersonalised information is exchanged between individual agencies outside of the data hub arrangements form ISP 3 is used.

6.8 Criminal Justice Agencies including the LCJB

As well as those agencies involved in CSP activity, agencies represented on the Local Criminal Justice Board are also legitimate requesters and sharers of information under this protocol. This includes the Youth Offending Service, Probation Service, Crown Prosecution Service and Drug and Alcohol Action Teams.

6.9 Health and social care agencies

Health, social service and other care agencies have a key role in information sharing in the crime and disorder area but information sharing in this area is particularly influenced by the series of legal judgements that have defined the duty of confidentiality.

A number of Information Sharing Protocols exist in the health, children and young people and adult care sectors. Whilst securing subject consent will normally be necessary for sharing personal information held by the health and care sector agencies, this may not always be possible or appropriate in the crime and disorder context. The expectation is that Designated Officers in these areas will make specific judgements on individual cases based on necessity and severity.

7 Information Sharing for Particular Schemes

7.1 Criminal Justice Integrated Team (CJIT)

Integrated Offender Management (IOM) targets young and adult offenders in the community (both those on statutory supervision and those who are not) who present the highest risks to their communities, especially those short sentence offenders released from prison under no statutory supervision. It seeks to build on the work already done to 'prevent and deter' and 'catch and convict' offenders by enhancing work done to 'rehabilitate and resettle' them. The strength of the CJIT is to manage offenders in the community through multi-agency approaches, ensuring offenders are assisted in their rehabilitation through positive support, but also to ensure that deterrent, sanctions and enforcement measures are quickly activated for those offenders that do no not comply.

CJIT approaches draw on the resources and support of ***all*** relevant partners to supervise, resettle and rehabilitate young and adult offenders. Multi-agency problem solving for identification, assessment, management and enforcement means that information sharing is a key part of the process. For more information on information sharing for CJIT see Guidance Notes page 36.

7.2 Prolific and other Priority Offender Scheme

The PPO scheme includes three strands – Prevent and Deter, Catch and Convict, and Rehabilitate and Resettle for which Criminal Justice agencies are primarily responsible. Protocols and secure information exchange mechanisms have been put in place to meet the requirements in respect to prolific and other priority offenders in the Catch and Convict and Rehabilitate and Resettle strands.

The third strand – Prevent and Deter – is likely to engage a wider range of agencies in information sharing around identified young people and, whilst this ISP will need to be responsive to the requirements of the other two strands, the exchange in respect of Prevent and Deter initiatives will be covered by this ISP and subject to similar mechanisms as multi-agency/problem-solving groups.

7.3 Multi-Agency Risk Assessment Conferences

Multi-Agency Risk Assessment Conferences (MARAC), identify victims of domestic abuse who are most at risk of experiencing violence in the future. The MARAC is a forum that brings agencies together to agree joined up action to prevent further harm to survivors of domestic violence and their children. It aims to reduce risk of serious harm or homicide by identifying risk factors and supporting survivors.

A multi-agency partnership approach is necessary in order to meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs of those experiencing domestic abuse. Sharing information through the MARAC enables agencies to act from a better factual understanding of the situation and the risks faced by the person experiencing domestic abuse and any children. For more information on information sharing for MARACs see Guidance Notes page 37.

7.4 Troubled Families

The Troubled Families Programme has been developed to transform the way in which we deliver services to an identified cohort of families. The innovative and transformational approach provided successful sustainable outcomes for families with significant cost benefits.

This early help approach now includes two of the following indicators listed below:-

a) Parent/ and or children involved in crime or anti-social behaviour (ASB)
b) Children who do not attend school regularly
c) Children who need help
d) Unemployed adults / at risk of financial exclusion and young people at risk of worklessness
e) Families affected by domestic abuse
f) Parents and children with a range of health problems

8. Security

8.1 General principles

Ensuring that personal information is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access is the seventh principle of the Data Protection Act 1998. ISO27001 provides a baseline for security arrangements. Partners should ensure they have appropriate security in place and arrangements to monitor these.

A key issue, especially for electronic documentation, is the consistent use of encryption and secure information exchange. Unguarded exchange of personal information may not only infringe the rights of the individual subject or others that may be identifiable from the information, but also compromise the organisations sharing information or jeopardise any proceedings or legal measures based upon that information.

With remote working come additional risks due to the use of unencrypted flash drives, memory sticks and laptops. Agencies party to this ISP must ensure all personal data is held securely and adequately protected from unauthorised disclosure to ensure they meet the requirement of Principle 7.

Level A partners sharing personalised information are responsible for ensuring that laptops, drives or removable electronic media containing personal information used for remote working are encrypted, and have Home Office approved levels of security. To comply with national guidance encryption should be at least 256 bit.

Recent Home Office guidance with respect to third party suppliers suggests that:

a) No unencrypted laptops or drives or removable electronic media containing personal information should be taken outside secure office premises.
b) No transferring of any protected personal information from Home Office approved systems to third party suppliers owned laptops, PCs, USB keys, external drives and any other electronic media is permitted.

8.2 Secure information exchange

The Guidance Notes provide detailed advice and checklists on secure information exchange. The non-electronic means covered are post, fax, and verbal or paper exchange.

Electronic exchange can be the most secure and auditable means of exchanging information provided this is done using suitably secure technology. Standard e-mail, even with encryption, is not generally sufficiently secure to protect personal information.

Personal information should only be exchanged electronically using a secure messaging system and it is recommended that only those partners identified as Level A partners (see section 5.4), do so. See guidance notes pages 39-43.

8.3 Information exchange at multi-agency/problem solving groups

Multi-agency/problem solving meetings, where personal information is exchanged, must ensure that they maintain the security needed to operate safely within the legislative constraints. Key elements include a signatory form for use at each meeting to confirm attendance and compliance with data protection principles and this ISP. This is in the Guidance Notes (page 23)

Attendees at these meetings must also ensure that controls applied to agenda and minute documents are as secure as those used for requesting and securing personal information, since these will often name the individuals being considered and contain elements of the information contributory to the decision making process. Records of meetings and personal information must be subject to the principles set out in this ISP, particularly in relation to purpose and retention.

The most effective way to achieve this will be for each relevant group to identify a suitable Designated Officer who can act as an information and record manager on behalf of the group and ensure that information is kept securely and retained no longer than is necessary.

8.4 Secure information storage and retention

The Guidance Notes include advice on how information can be held securely and managed effectively to ensure disposal once the specific purpose has been fulfilled. The essence of this guidance is that:

a) Paperwork must be dated, suitably marked to indicate its sensitivity, and organised
b) Electronic files should be dated, encrypted if stored on any drive with general access, and viewed through a PC with password protection

c) Verbally exchanged information should be secure from eaves-dropping and recorded / validated as soon as possible. Verbal information should be subject to the same considerations as written, and should not be exchanged unless both parties are satisfied that the request is legitimate and there is a good reason for not pursuing a written route.

All records should be managed and reviewed to ensure that currency is maintained and that nothing is retained longer than required for the specific purpose that led to its exchange.

Paper records should be cross shredded and electronic records should be double deleted. All agencies should have internal procedures regarding data protection and requests which should also be observed.

9. Data Standards

BS7666 is the standard for describing locations such as addresses, rights of way and streets. Most information in the public sector has a location element to it so it is appropriate to use the BS7666 standard in order to convert disparate data sets from different systems and agencies.

10. Indemnity

Home Office guidelines state that:

> "As protocols are not legally-binding documents, it is wrong to assume that mention of indemnity clauses in any protocol would place all signatories beyond legal challenge, following a breach or disclosure of certain sensitive information."

In line with this guidance an indemnity clause has not been included in this document and all issues should be resolved on a case by case basis.

11. Information breaches

Individual Community Safety Teams cannot be held responsible for breaches of this protocol and complaints and breaches should be dealt with by utilising signatories' own organisations' established policies and procedures for breaches and complaints made in relation to any legislation in connection with information exchange.

Any disclosure of information by an employee which is made in bad faith or for motives of personal gain will be the subject of an inquiry by the respective employing agency and may be subject to criminal investigation. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents. Any misuse of information or breach of the ISP should be notified to the relevant agencies immediately.

12. Subject and Third Party Access

Under the terms of the Data Protection Act, any individual has the right to request access to information held about them (subject to exemptions) and this would include information held for community safety purposes. An individual may make a Subject Access request under the provisions of the DPA using the existing mechanisms and forms of each agency.

If an agency receives a subject access application, they need to consider whether the information can be provided, or whether an exemption under the Data Protection Act needs to be applied to enable the request to be denied. Examples where an exemption might apply would include where the information cannot be supplied without identifying a third party, or where disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

Where a third party can be identified from the information, the Data Controller is not obliged to comply with the request unless:

- The other individual has consented in writing to the disclosure of the information to the person making the request, or;
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

The underlying principle of the protocol is that an agency will always retain ownership of the personal information it discloses to another member of the partnership. The identity of the originator must therefore be recorded against the relevant information. A recipient of such information must obtain the consent of the original data owner before making a further disclosure.
If the personal information requested is identified as belonging to another agency, it will be the responsibility of the receiving agency to contact the data owner to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act. If, in the judgement of the Data Controller there are grounds for an exemption under the provisions of the Data Protection Act, a mandate endorsing this decision should be obtained from the agency's Data Protection Officer using Form ISP5.

All agencies need to co-operate speedily to ensure that requests are met within the statutory time period set out in the Data Protection Act. Where agencies consult with other agencies in relation to releasing the information they hold the request must be made within five days of the subject access request. The agency then has twenty days to respond to the enquiry so that the agency receiving the original subject access request can comply with the 40 day limit set within the Act. The final decision to release the information rests with the agency that the information has been requested from in line with Data Protection regulations. It is suggested that a general principle of removing third party information is applied when releasing information.

It should be noted that information supplied to the Police and the Crown Prosecution Service becomes the property of these agencies and therefore other agencies will not need to be contacted in regards to the release of the information.

For more information please see page 46 of the Guidance Notes.

13. Guidance Notes

Guidance notes have been produced in conjunction with this protocol and will be issued to all Designated Officers. The Guidance Notes and the Protocol will be available through each Community Safety Partnership website - where updates will be posted and Designated Officers informed of any changes. Any changes or updates to the Guidance Notes will be agreed by the SSP Executive Group.

Legal advice on this agreement should be sought in any case of doubt.

Each party to this agreement will introduce their own arrangements to test that this agreement, its associated working practices and legal requirements are being adhered to.

14. Confidentiality Agreement

The information will only be used for the purpose for which it was requested, and it will be securely, exchanged, stored and destroyed when no longer required. All agencies that are part of the information sharing process will, upon signing this protocol, be bound to comply with its terms.

15. Commencement & Review

This document was reviewed in October 2015. It will be subject to further review in October 2016, and then every twelve months or sooner if relevant developments or issues dictate.

Appendix 1 Datasets specified under the Police and Justice Act 2006

Organisation	Datasets (for the area)
Police	1. Records on anti-social behaviour, transport and public safety/welfare **incidents** recorded according to the National Incident Category List. Whatever information is recorded about the time, date, location and category of each incident must be disclosed. 2. **Crime records** recorded according to the Notifiable Offences list. Whatever information is recorded about the time, date, location and sub-category of each crime must be disclosed.
Fire and Rescue	3. Records on **deliberate fires**, whether it was a deliberate primary fire (not in a vehicle), a deliberate secondary fire (not in a vehicle) or a deliberate fire in a vehicle. In addition, records on **incidents of violence against employees** and records of fires attended in dwellings where **no smoke alarm** was fitted. For all these records, whatever information is recorded about the time, date and location of the fire must be shared. 4. Records on **malicious false alarms**. Whatever information is recorded about the time and date of each call and the purported location of those alarms must be shared.
Local Authority	5. Records on **road traffic collisions**. Whatever information is recorded about the time, date, location and the number of adults and children killed, seriously injured and slightly injured in each road traffic collision must be shared. 6. Records on **fixed term and permanent school exclusions**. Whatever information is held about the age and gender of the pupil, the name and address of the school from which they were excluded and the reasons for their exclusion must be shared. 7. Records of **racial incidents**. Whatever information is held about the time, date and location of each incident must be shared. 8. Records of **anti-social behaviour incidents** identified by the authority or reported by the public. Whatever information is held about the category, time, date and location of each incident must be shared.
NHS /CCG	9. Records on various categories of **hospital admissions**. The relevant admissions are those relating to the following blocks within the International Classification of Diseases: a) assault (X85-Y09); b) mental and behavioural disorders due to psychoactive substance use (F10-F19); c) toxic effect of alcohol (T51); and d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or evidence of alcohol involvement determined by level of intoxication (Y91).For each record, whatever information is held about the date of the admission, the sub-category of the admission and the outward part of the postcode (the first part of the postcode, before the space which separates it from the second part) of the patient's address must be shared. 10. Records of admissions to hospital in respect of **domestic abuse**. Whatever information is held about the date of the admission and the outward part of the postcode of the patient's address must be shared. 11. Numbers of **mental illness outpatient first attendances** and **persons receiving drug treatment**.
Ambulance Service	12. Records of **ambulance call outs** to crime and disorder incidents. Whatever information is held about the category, time, date and location of each ambulance call out must be shared.

The Police and Justice Act 2006 specifically excludes any personal information from this duty to disclose. This means information which can identify a living individual, either by itself or in combination with other information held, or likely to be held, by the relevant authority. Where an incident is recorded as a domestic incident, for example, sharing precise location information may, in some circumstances, be sufficient to identify a living individual. In such instances, the duty does not apply. Subject to complying with other legal obligations such as the common law of confidentiality for information from ambulance callouts, the authority may

still choose to disclose this information to the other Section 115 relevant authorities, (Crime and Disorder Act 1998) who should treat it as personal information. Alternatively, the authority may choose to share less specific location information so that the dataset contains exclusively depersonalised information. In the case of ambulance callouts, this should be the outward part of the postcode only.

Appendix 2 Authorised Signatory Form

COMMUNITY SAFETY INFORMATION SHARING PROTOCOL

SECTION ONE
(details of organisation wishing to become a signatory to the protocol)

Name of organisation:

Address:

Local Authorities covered by organisation:

SECTION TWO:
(to be completed by the chief officer of the organisation wishing to become a signatory)

I would like this organisation to become a signatory to the Community Safety Information Sharing Protocol. I sign this form with the understanding that my organisation will comply fully with the conditions of the Protocol.

Name:

Position:

Signature:
Date:

TFTC Individual Consent

Appendix 3 ISP1 - INDIVIDUAL CONSENT TO PERSONAL INFORMATION DISCLOSURE

DETAILS OF REQUESTING OFFICER	
Name	
Title and Agency:	
Address:	
Email:	
Telephone:	
Case Reference:	

Declaration:

I/We ……
(insert name of individual or person and if necessary any person signing on their behalf)

authorise

……
(insert name of relevant authority)

to share personal/sensitive personal data relating to myself with any requesting authority. These data will be limited to what is required for the purpose of:

I understand the personal data provided will not be used for any other purpose or further disclosed beyond those immediately involved in the joint undertaking without my further consent. The further data may be retained by the Requesting Authority for a period of time, limited to the authorised purpose, after which it will be destroyed.

Signed: _____ Date: _____
Data Subject

Signed: _____ Date: _____
Person responsible for data subject

Signed: _____ Date: _____
Agency representation

Appendix 4 Attendance and Compliance List

RESTRICTED (When complete)

Event / Meeting:
Date:
Time:
Location:

The persons listed who have attended this meeting have agreed that the overriding principle of sharing information is to prevent crime and disorder, anti-social behaviour and substance misuse, and apprehend and prosecute offenders in Stockton. Matters discussed at this meeting will remain confidential within the organisations attending this meeting unless otherwise agreed by the meeting and recorded within any action plan. Information shared is done so in compliance with the Safer Stockton Partnership Information Sharing Protocol. Any disclosure has to be agreed at the Meeting or by the chair of the Meeting. We further confirm that we represent agencies that are signatories to the Information Sharing Protocol and that we are Designated Officers authorised to share and exchange information as appropriate

The parties subject of the information sharing protocol agree that where an offence is alleged to have been committed, but there is insufficient evidence to proceed, it is not unlawful to release information but it must be done with a clear indication that there has not been a conviction nor has the evidence been tested in Court. It is important that organisations distinguish between fact and intelligence/opinion.

NAME	TITLE/ROLE	AGENCY	TEL	SIGNATURE

SECTION THREE:
(data protection)

You need to ensure that you have notified the Information Commissioners Office under the Data Protection Act to share information with other agencies for the purposes of the prevention or detection of crime and the apprehension or prosecution of offenders. This will need to be done through your Data Protection Officer or the individual in your organisation responsible for maintaining your Data Protection Notification.

On signing this form you are indicating that your Data Protection Notification has been checked and appropriately updated to reflect information sharing for this purpose.

Please record your Data Protection Register Entry Number here:

SECTION FOUR:
(Nomination of designated officers for information sharing)

Please provide the names and contact details of at least two designated officers for information sharing from your organisation. (You may nominate as many designated officers as are appropriate). In addition would you also identify a designated manager, who will be responsible for informing the Community Safety Team if the designated officers or their contact details change.

Designated Officer Manager
Name:
Position:
Address:

Email:
Telephone:

Designated Officer One
Name:
Position:
Address:

Email:
Telephone:
Fax:

Designated Officer Two
Name:
Position:
Address:

Email:
Telephone:
Fax:

Designated Officer Three
Name:
Position:
Address:

Email:
Telephone:
Fax:

Designated Officer Four
Name:
Position:
Address:

Email:
Telephone:
Fax:

Designated Officer Five
Name:
Position:
Address:

Email:
Telephone:
Fax:

Designated Officer Six

Position:
Address:
Email:
Telephone:
Fax:

Designated Officer Seven

Name:
Position:
Address:
Email:
Telephone:
Fax:

Appendix 5– Attendance & Compliance List

(NAME OF MEETING) Meeting
(Name of Household/Individual if appropriate)

Date

Attendance List

Declaration of agreement with information sharing and exchange principles
We, the undersigned, accept and understand that the principles of the legislation regulating the exchange of information apply to the content of this meeting principally: *Section 115 of the Crime and Disorder Act 1998*. We understand that information shared and exchanged at this meeting is for the specific purpose of dealing with crime & disorder related issues within the area covered by this multi-agency (Problem Solving Group/Joint Action Groups) name of group e.g. Domestic Abuse Medium Repeats group and may not be used for any purpose other than that for which it is intended. We further confirm that we represent agencies that are authorised to share and exchange information as appropriate.

Name	Organisation/Department	Signature

Appendix 6

Level A Partner Signatories

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Agency	
Signature	
Print Name	
Designation	

Level B Partner Sign Up

This ISP forms part of the framework for information sharing that is in place within the North East region. The protocol is complemented by and should be used in conjunction with the Safer Stockton Partnership Information Sharing Guidance Notes which provide more detailed information to support this Information Sharing Protocol.

This protocol conforms to Information Commissioners Office (ICO) guidance. The ICO enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations.

The purpose of sharing information within the Safer Stockton Partnership is to:

a) **Prevent crime and anti-social behaviour**
b) **Reducing crime, anti-social behaviour and the fear of**
c) **Apprehending and prosecuting offenders**
d) **Reducing re-offending**
e) **Increase public reassurance and reduce the fear of crime / asb**

In order to become a Level B signatory, the following information must be provided to the Safer Stockton Partnership:

- Organisation Name
- Information Sharing Lead
- ICO Registration details

Upon receipt of this information Safer Stockton Partnership will then issue a 'Level B Partner Sign-up Form' for the organisation to complete and return.

Level B signatories to this protocol agree to meet the standards outlined in Section 5 of the ISP. They commit to a positive and legal approach to information sharing, as defined in this document and guidance.