Safer Sunderland Partnership Information Sharing Protocol

Version 1.1 Date 29/12/2022
Updated Date August 2021
Updated Date February 2023

Contents

Acknowledgements

The Safer Sunderland Partnership (SSP) have adapted this Information Sharing Protocol from North East Community Safety Information Sharing Protocol developed by the Home Office.

1. Background and purpose of the protocol

This Information Sharing Protocol (ISP) is owned by the Safer Sunderland Partnership. Any enquiries about the content of the document should be directed to the Strategic Manager Community Safety & Safeguarding.

1.1 Background

This ISP forms part of the framework for information sharing that is in place within the Safer Sunderland Partnership. The protocol is complemented by the Safer Sunderland Information Sharing Guidelines and provides a strategic set of principles to be followed when sharing and/or jointly processing personal information. The Information Commissioner's Office (ICO) enforces and oversees the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act (FOIA), the Environmental Information Regulations (EIR), and the Privacy and Electronic Communications Regulations (PECR). This protocol conforms to the ICO guidance which is available at:Data sharing: a code of practice | ICO

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

1.2 Purpose

The purpose of sharing information[1] within Community Safety Partnership (CSP) is:

a) Preventing crime and disorder, anti-social behaviour and substance misuse
b) Reducing crime and disorder, anti-social behaviour and substance misuse
c) Apprehending and prosecuting offenders
d) Reducing re-offending
e) Enhancing community safety and cohesion (tension monitoring)
f) General community safety related information analysis

The ISP seeks to:

a) Facilitate the secure exchange of depersonalised and personalised information between signatory agencies
b) Govern the use and management of information by Community Safety Partnerships 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 environment, tackling substance misuse and adult and youth offending.
c) Support the actions of the CSPs multi-agency/problem solving groups involved in tackling crime, anti-social behaviour and substance misuse.
d) Assist the work of Sunderland Drug and Alcohol services to tackle substance misuse.

[1] For the purposes of this protocol the term "information" will be used to include "personal data", as defined in the UK GDPR and "information " as defined in the Crime and Disorder Act and Police and Justice Act.

e) 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.
f) Assist the work of the Local Criminal Justice Boards.
g) Assist the work of the UK border agency.
h) Support the development of secure information exchange in response to Integrated Offender Management (IOM) and Prolific and Priority Offender schemes.
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 community fire safety.
k) Enable statutory authorities to more effectively meet their obligations under Section 17 of the 1998 Crime and Disorder Act and the amendments made by the Police and Justice Act 2006.
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.

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 covered by their own Information Sharing Protocol, however many of the underlying principles and governance will be similar.

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 an exchange of information between one or more individuals or agencies.

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 affecting 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.

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.

Controller
Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Disorder
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.

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

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.

Law Enforcement Purposes
Law Enforcement Purposes means the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Personal Data (as defined under Article 4 of the UK GDPR)
Personal Data means any information relating to an identified or identifiable natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (See Guidance Notes on pages 7 to 11for rules on how Personal Data must be processed).

Personal Data Breach
Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Special Category Personal Data (as defined under Article 9 of the UK GDPR)

This is information describing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) membership of a trade union
e) physical or mental health or condition
f) sexual life or sexual orientation
g) genetic data or
h) biometric data for the purpose of uniquely identifying a natural person.

4. The legal framework for sharing and exchanging information

4.1 Sharing Information

4.1.1 Crime and Disorder Act (1998)

Section 115 of the Crime and Disorder Act 1998 provides a legal basis (not a statutory duty) for information sharing with relevant authorities where it is necessary for fulfilling duties contained in the Act. There is a wide range of activities in which the sharing of personal information is not only useful but legally permissible, particularly where decisions regarding particular interventions with individuals are being discussed. This power however does not override other legal obligations such as compliance with the UK GDPR, DPA 2018, 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.

4.1.2 Criminal Justice and Court Services Act (2000)

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

4.1.3 Police and Justice Act (2006)

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

The Police and Justice Act 2006 also places a statutory duty on the strategy group of all Community Safety 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 responsible authorities and other agencies named under Section 115 of the Crime and Disorder Act 1998, including personal information. A statutory duty has also been placed on each responsible authority to nominate a designated liaison officer whose role is to facilitate the sharing of information with other partners.

4.1.4 Counter-Terrorism and Border Security Act 2019

This Act enables local authorities, as well as the police, to refer persons at risk of being drawn into terrorism to local ("Channel") panels. A Channel panel helps to deliver the aims of the Prevent strategy by ensuring that individuals who are identified as being at risk of being drawn into terrorism are given appropriate advice and support so that they may turn away from radicalisation.

4.1.5 Other relevant Acts

Whilst the legislation highlighted in sections 4.1.1 to 4.1.4 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

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

- Police and Criminal Evidence Act 2001

4.2 Legislation governing the sharing of information

4.2.1 The UK GDPR and the DPA 2018

The UK GDPR, together with the DPA 2018 set out the data protection framework in the UK. This legislation sets out the key principles, rights and obligations for processing of Personal Data. Processing for Law Enforcement Processing is covered under Part 3 of the DPA 2018 and this needs to be read alongside certain applicable Articles of the UK GDPR. See further details below under 'Law Enforcement Processing'.

Unless exempt, all UK organisations that process personal data are required to register with the ICO and pay an annual fee. As mentioned above, the ICO is the regulator of data protection in the UK and is an executive non-departmental public body sponsored by the Department for Digital, Culture, Media and Sport. **Each agency under the Safer Sunderland Partnership must ensure that they are registered with the ICO [4] before sharing information under this protocol.**

It is important that the parties to the Safer Sunderland Partnership are familiar with the key elements of the UK GDPR, including the data protection principles, the lawful bases and the conditions for processing Special Category Personal Data, as set out below.

UK GDPR

Article 5 of the UK GDPR outlines seven principles relating to the processing of Personal Data. It provides that Personal Data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation')

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

[4] An independent official appointed by the Crown to oversee the Data Protection and Freedom of Information Acts – see their website at https://ico.org.uk

accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(g) The controller shall be responsible for, and **be able to demonstrate compliance** with, (a) to (f) ('accountability')

Lawful bases for processing Personal Data
The UK GDPR provides that Personal Data shall only be processed if a lawful basis is identified under Article 6 of the UK GDPR. Those lawful bases are:

Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; ('consent')
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ('contract')
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; ('legal obligation')
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; ('vital interests')
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; ('public task')
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. ('legitimate interests')

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for processing Special Category Personal Data
Furthermore, Article 9 of the UK GDPR provides that the processing of Special Category Personal Data **shall be prohibited unless one of the following applies:**

a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and subject to certain conditions

e) processing relates to personal data which are manifestly made public by the data subject

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject domestic law;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards

i) processing is necessary for reasons of public interest in the area of public health such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy domestic law;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

For more information, please see Lawfulness | ICO

4.2.1.1 Law Enforcement Processing

As mentioned above, the DPA 2018 makes provision for processing of Personal Data for Law Enforcement Purposes. In particular Part 3 of the DPA 2018 applies to 'Competent Authorities' processing personal data for this purpose.'.

Section 30(1) provides that 'Competent Authorities' means *'a person specified or described within Schedule 7 of the DPA 2018 and any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for law enforcement purposes'*.

For example, local authorities when prosecuting trading standards offences would fall within this definition.

Section 31 of the DPA 2018 defines 'Law Enforcement Purposes' as:

"The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"

The principles Part 3 of the DPA 2018 are broadly the same as those in Article 5 of the UK GDPR (outlined in section 4.2.1 above), and are compatible so Competent Authorities can manage processing concurrently across the two regimes.

However, the transparency requirements (e.g as at Article 5, Principle (a) in 4.2.1 above) are not as strict, due to the potential to prejudice an ongoing investigation in certain circumstances. Similarly, data subjects have fewer rights and the rights that they do have are not as broad as they are under the UK GDPR.

This lack of transparency, and the narrower range of data subject rights (see 4.2.1.2 below), are counter-balanced in DPA 2018 by the requirement to implement robust boundaries when processing for Law Enforcement Purposes. These include:

- Maintaining an **Appropriate Policy Document** where processing special category information (see 4.2.1 above) for Law Enforcement Purposes
- Maintaining **Logs** of the collection, use and disclosure of data. This applies to requests for re-use of data within an organisation, as well as external requests received from partner organisations
- Maintaining Records of Processing Activity (**ROPA**)
- Adopting a **Categorization Methodology** to ensure there is a clear distinction between victims, witnesses, suspects and persons convicted.
- Maintain a **Retention schedule** outlining retention and disposal periods for data processed for law enforcement purposes

4.2.1.2 Right to be informed (privacy notices), right of access (subject access requests) and other subject rights

Schedule 2, Part 1, Para 2 of the DPA 2018 states that the following provisions under the UK GDPR:

- Article 13(1) to (3) (personal data collected from data subject: information to be provided); ***Privacy Notice***
- Article 14(1) to (4) (personal data collected other than from data subject: information to be provided); ***Privacy Notice***
- Article 15(1) to (3) (confirmation of processing, **access to data** and safeguards for third country transfers);
- Article 16 (right to **rectification**);
- Article 17(1) and (2) (right to **erasure**);
- Article 18(1) (**restriction** of processing);
- Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
- Article 20(1) and (2) (right to **data portability**);
- Article 21(1) (**objections** to processing);

do **NOT** apply to personal data processed for any of the following purposes—

(a)the prevention or detection of crime,
(b)the apprehension or prosecution of offenders, or
(c)the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

In terms of the right to be informed (privacy notices), part 3, Chapter 3 of the DPA 2018 imposes general duties on Competent Authorities processing personal information for Law Enforcement Purposes to make limited information available to data subjects and, in terms of data subjects' rights, it confers a narrow range of rights on the data subjects. These rights can be further restricted where considered necessary and proportionate to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security;
- protect the rights and freedoms of others.

If such a restriction is applied, the Competent Authority y must **record the reasons for a decision to restrict**. This is in addition to the recording requirements outlined in 4.2.1.1 above

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 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 judgments 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 judgments have identified a number of exceptions:

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

Where information is held in confidence e.g. as is the case with personal information provided to the National Health Service and medical practitioners by patients, the consent of the individual concerned should normally be sought prior to information being disclosed. Where consent is withheld or is unobtainable, designated officers should assess on a case-by-case basis, whether disclosure is necessary to support action under the Crime and Disorder Act and 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, the principles have developed and there are now eight general principles for the safe handling of personal-identifiable information, that provide the guidelines to which the NHS works. The principles are:

1. Justify the purpose for using confidential information.
2. Use confidential information only when it is necessary.
3. Use the minimum necessary confidential information.
4. Access to confidential information should be on a strict need to know basis.
5. Everyone with access to confidential information should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information for individual care is as important as the duty to protect patient confidentiality.
8. Inform patients and service users about thow their confidential information is used.

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 UK GDPR or the DPA 2018 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 UK GDPR and the DPA 2018 continues to govern access to personal 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

FOIA. Their advice should be sought in the event of any questions arising about the FOIA,.

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 FOIA 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.

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 in a CSP. Under Section 5 of the Crime and Disorder Act 1998 the following organisations are named as Responsible Authorities:

a) District/Borough council, unitary authority or County Council.
b) Police Force (Chief Police Officer).
c) Police Authority (as amended under the Police Reform Act 2002).
d) Fire Authority (as amended under the Police Reform Act 2002)
e) Primary Care Trusts (as amended under the Police Reform Act 2002).
f) Probation Trusts

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 comprise of 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.

Responsible Authorities are required to work in co-operation with probation boards, 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 Substance misuse services. 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 CSP 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 substance misuse).

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 a person to disclose to a "relevant authority" where the person does not usually have the power to do so, but the disclosure is necessary or expedient for the purposes of any provision of the Crime and Disorder Act.

Relevant authorities are defined as:

a) Police forces and police authorities
b) Local authorities (such as district, borough & county councils)
c) Probation Boards/Trusts
d) Fire and rescue authorities
e) Health authorities
f) Primary Care Trusts
g) 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

Level A means partners that are empowered under the Anti-Social Behaviour Act to take out Anti-Social Behaviour Orders. Registered Social Landlords are also designated as cooperating bodies [insert brief description of criteria for level A partners].
Level B means partners that are less likely to take a central role with the processes for sharing personalised information but may use the protocol for sharing depersonalised information This ISP designates two levels of agency determined by the extent of their involvement with CSP 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 below). Level A partners are:

NEAS
North East Ambulance Service NHS Trust
Bernicia House
Goldcrest Way
Newburn Riverside
Newcastle upon Tyne
NE15 8NY

North East Strategic Health Authority,
Riverside House,
Goldcrest Way,
Newcastle Upon Tyne,
Tyne and Wear,
NE15 8NY

Northumberland Tyne and Wear NHS Foundation Trust
St Nicholas Hospital
Jubilee Road
Gosforth
Newcastle upon Tyne
NE3 3XT

Tees, ESK and Wear Valleys
West Park Hospital
Edward Pease Way
Darlington
County Durham

DL2 2TS

HMPS North East Area Office
2 Artemis Court
St Johns Road
Meadowfield
Durham
DH7 8XQ

Her Majesty's Court Service
Sunderland Magistrates Court
Gilbridge Avenue
SR1 3AP

Victim Support
3 Toward Road
Sunderland
SR1 2QG

Gentoo Sunderland
2 Emperor Way
Doxford International Business Park
Sunderland
SR3 3XR

Bernicia Housing Group
Cheviot House
Beaminster House
Kingston Park
Newcastle-upon-Tyne
NE3 2ER

Three Rivers Housing Association
Head Office
Three Rivers House
Abbeywoods Business Park
Pity Me
DH1 5TG

Believe Housing
Coast House
Spectrum 4
Spectrum Business Park
Seaham
County Durham
SR7 7TT

HOME
Home Tenancy Enforcement
Woodstone House
Woodstone Village
Co/Durham
DH4 6BQ

Housing Associations and other Registered Social Landlords are designated as Level A partners since they are empowered under the Anti-Social Behaviour Act to take out Anti-Social Behaviour Orders. Registered Social Landlords are also designated as cooperating bodies. Where housing authorities are seeking injunctions under the Housing Act the separate protocols established between each RSL and the Police should govern the process for information exchange.

Increasingly voluntary sector agencies are providing key support services essential for the functioning of CSPs and Drug and Alcohol Services. Where possible 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 or covered in separate information sharing protocol arrangements by their commissioning body.

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.

Level B Partners include

Youth Consortium

Sunderland Business Improvement District (BID)

Washington Galleries (LCP Properties)
Galleries Shopping Centre
Washington
Tyne & Wear

5.5 Responsibilities of signatories

a) It is the responsibility of signatories to ensure that:
b) They are correctly registered with the Information Commissioner for sharing personal information
c) The data protection principles are upheld
d) The information shared is kept secure and confidential
e) Information is accurate and up to date
f) Realistic expectations prevail from the outset
g) Professional ethical standards are maintained
h) A mechanism exists by which the flow of information can be controlled
i) Appropriate staff training is provided on this protocol
j) Adequate arrangements exist to test adherence to the protocol

k) Records are maintained of decisions to share or withhold information
l) 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. 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 6.2 for explanation of this role) are conversant with the ISP and their responsibilities.
More information on meeting the responsibilities of this ISP is contained in the Guidance Notes supplied with this document.

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 UK GDPR and the DPA 2018 requirements around information exchange within and outside the UK, 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 UK GDPR and the DPA 2018. As a result, personal information needs to be processed fairly and lawfully, and should not be processed unless:

- a lawful basis under Article 6 of the UK GDPR applies, and,
- for special category information, a condition under Article 9, together with a condition under Schedule 1 to the DPA 2018, (where applicable), is met,

For more information please see Data sharing: a code of practice | ICO).

The UK GDPR and the DPA 2018 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. Before doing so, it is important that a lawful basis under Article 6 is identified and, if necessary, condition(s) under Article 9 and Schedule 1 to the DPA 2018 (where necessary) is/are satisfied in order to share information. In some situations, it may be necessary to rely upon an exemption under schedule 2, Part 1 of the DPA 2018 applies. For more information please see Data Protection Act 2018 (legislation.gov.uk).

Any disclosure or sharing of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidentiality (see Data sharing: a code of practice | ICO), 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, if possible and appropriate, written consent from any identifiable third party should be sought, a sample form is provided in (ISP Form 1, pages 25 and 26 of the Guidance). It is recommended that advice is taken from your organisation's Data Protection Office or Legal Service where the disclosure of information would include any third party information.

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

A **log** of disclosure must be maintained in line with the requirements of Section 62 of the DPA 2018, to include:

(a)the justification for, and date and time of, the disclosure, and
(b)so far as possible—
(i)the identity of the person who disclosed the data, and
(ii)the identity of the recipients of the data.

Disclosure applies to requests both from within an organisation and from external partners, and where IT systems do not allow for automatic logging, manual logs must be created.

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 Designated Officers

The signatories to this protocol will nominate as many Designated Officers as are needed 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 must submit the request through their own agency's Designated Officer.

The Guidance Notes include a checklist for Designated Officers (pages 18-19) 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.

Designated Officers will be identified within each agency.

6.3 Designated Managers

The signatories to this protocol will nominate one individual from their organisation to be responsible for the management of their Designated Officers. Their primary role will be to identify appropriate nominated designated officers.

Under the Police and Justice Act 2006 Responsible Authorities now have a statutory duty to nominate a Designated Liaison Officer whose role is to proactively facilitate information sharing with other partners. The Designated Manager should also take this role and be responsible for proactively promoting information sharing between agencies and ensure compliance with the minimum information sharing requirements for the responsible authorities.

6.4 Multi-agency/problem solving groups

Multi agency/problem solving groups consist of relevant agencies brought together to address community safety issues. Sunderland LMAPs group members sign a confidentiality sheet prior to meetings. 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 should be recorded.

6.5 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,

6.6 Criminal Justice Agencies including the Local Criminal Justice Board (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 for example Youth Offending Service, Probation Service, Crown Prosecution Service.

6.7 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 Integrated Offender Management

Integrated Offender Management (IOM) approaches young and adult target 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 IOM 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.

IOM 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 IOM see Guidance Notes page 33.

7.2 Prolific and Priority Offender Schemes

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 or any children experiencing domestic abuse. For more information on information sharing for MARACs see Guidance Notes page 34.

8. Security

8.1 General principles

Applying appropriate technical and organisational measures so that personal information is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, and against accidental destruction, loss, or damage is the sixth principle of the UK GDPR. 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 there is an issue about storing personalised information on flash drives/memory sticks and of encryption. Some agencies such as Probation have Home Office approved data secure memory sticks and encrypted laptops.

Level A partners sharing personalized 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 (e.g. NHS.net, Criminal Justice Secure Mail: CJSM; GSX) and it is recommended that only those partners identified as Level A partners (see section 5.4), do so. See guidance notes pages 38

8.3 Information exchange at multi-agency/problem solving groups

Multi-agency/problem solving meeting 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. A sample form is in the guidance Notes (page 27)

Attendees at these meetings must also ensure that controls applied to agenda and minute documents as 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.

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 eavesdropping 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

Complaints and breaches should be dealt with by utilising signatory' organisations' established policies and procedures for breaches and complaints, liaising with partner organisations where necessary.

Any unauthorised 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.

If an information breach amounts to a Personal Data Breach, the party responsible shall invoke its Personal Data Breach Procedure immediately.

12. Subject and Third Party Access (see also 4.2.1.2)

Under the terms of the UK GDPR and the DPA 2018, 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 UK GDPR and the DPA 2018 using the existing mechanisms and forms of each party to the Safer Sunderland Partnership, if they are a controller.

If a controller receives a subject access application, they need to consider whether the information can be provided, or whether any of the exemptions under Schedules 2, 3 and 4 of the DPA 2018 apply. An example of where an exemption might apply would be where disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

Further, the DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except where:

- 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.

In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—

(a)the type of information that would be disclosed,

(b)any duty of confidentiality owed to the other individual,

(c)any steps taken by the controller with a view to seeking the consent of the other individual,

(d)whether the other individual is capable of giving consent, and

(e)any express refusal of consent by the other individual.

If the personal information requested is identified as originating from another controller, it will be the responsibility of the receiving controller to contact the original controller to advise that it will release the information *unless* the original controller identifies an exemption under the provisions of the DPA 2018. If, in the judgement of the original controller there are grounds for an exemption, a mandate endorsing this decision should be obtained from the original controller's Data Protection Officer. A sample form is provided as in Form ISP5.

All controllers need to co-operate speedily to ensure that requests are met within the statutory time period set out in the UK GDPR and the DPA 2018. Where receiving controllers need to consult regarding releasing the information they hold, the request should be made within five days of receipt of the subject access request. The original controller then has twenty days to respond to the consultation request so that the receiving controller can comply within the one calendar month limit set within the legislation. The final decision to release the information rests with the *receiving* controller that the information has been requested from in line with data protection legislation.

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 43 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 Sunderland City Council 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 Safer Sunderland Partnership.

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

The commencement date of this protocol will be: 02/08/2012 it will be reviewed annually 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 / PCT	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.

Schedule 9, Para 7 of the Police and Justice Act 2006 amends Section 115 of the Crime and Disorder Act 1998 to state:

"Any person who, apart from this subsection, would not have power to disclose information— (a) to a relevant authority; or (b) to a person acting on behalf of such an authority, shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act."

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, 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

SAFER SUNDERLAND PARTNERSHIP INFORMATION SHARING PROTOCOL

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

Name of organisation: _____

_____

Address: _____

_____

_____

_____

Local Authorities covered by organisation: _____

_____

_____

_____

_____

Signature: _____

_____

Date: _____

_____

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 SAFER SUNDERLAND PARTNERSHIP Information Sharing Protocol. I sign this form with the understanding that my organisation will comply fully with the conditions of the Protocol.

Name: [redacted]
Position: Leader of the Council (CSP Chair)
Organisation: Sunderland City Council
Address: City Hall

Signature:
Date:

Name: [redacted]
Position: Director of Children Services & Chief Executive TfC
Organisation: Together for Children
Address: Sunderland

Signature: [redacted]
Date: 2/03/2023

Name: [redacted]
Position: Executive Director Health, Housing & Communities
Organisation: Sunderland City Council
Address: City Hall

Signature:
Date:

Name: [redacted]
Position: Director Adult Services
Organisation: Sunderland City Council
Address: City Hall

Signature:
Date:

Name: [redacted]
Position: Chief Inspector
Organisation: Northumbria Police
Address:

Signature:

Date:

Name:
Position:
Organisation: Tyne and Wear Fire and Rescue Service
Address:

Signature:
Date:

Name: Wendy Proctor
Position: Designated Nurse Adult Safeguarding

Organisation: North East & North Cumbria Integrated Care Board
Address: Pemberton House, Sunderland

Signature:
Date:

Name: [redacted]
Position: Head of Sunderland Probation Delivery Unit
Organisation: National Probation Service
Address: The Lightbox, Quorum Business Park, NE12 8EU

Signature:
Date:

Level B Partner

Name:
Position:
Organisation:
Address:

Signature:
Date:

SECTION THREE:
(Data protection)

You need to ensure that you have registered with the Information Commissioners Office under the Data Protection Act. This should 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 you have registered with the ICO.
