South West Regional Serious Violence and Contextualised Safeguarding Information Governance Framework (FINAL v1.0)

Contents

[1. Introduction and context 3](#_Toc78401629)

[2. Aims of the framework 5](#_Toc78401630)

[3. How the framework will work in practice: 5](#_Toc78401631)

[4. Principles for sharing data 6](#_Toc78401632)

[5. Principles for safeguarding: 7](#_Toc78401633)

[6. Principles for purposes other than safeguarding: 8](#_Toc78401634)

[7. Process for establishing initiative specific data sharing arrangements 10](#_Toc78401635)

[8. Organisational commitments 12](#_Toc78401636)

[9. Sharing partner assurances 12](#_Toc78401637)

[Appendix 1. Tools to support sharing initiatives 13](#_Toc78401638)

[Appendix 2. Reference materials: the components of data sharing. 15](#_Toc78401639)

[Appendix 3. Reference materials: Legal gateways supporting data sharing 18](#_Toc78401640)

[Appendix 4. Application of UK GDPR Article 6 and 9 processing conditions to uses of data for purposes related to reducing serious violence and safeguarding concerns 26](#_Toc78401641)

[Appendix 5. Qualifying Standard (Example) 29](#_Toc78401642)

[Appendix 6. Signature of agreement to framework 30](#_Toc78401643)

# Introduction and context

“Violence is preventable, not inevitable”[[1]](#footnote-1)

In April 2018 the Government published its [Serious Violence Strategy](https://www.gov.uk/government/publications/serious-violence-strategy) in response to increases in knife crime, gun crime and homicide across England. The strategy represented a step change in how to think and respond to serious violence, establishing a new balance between prevention and law enforcement. It declared a call to action to partners from across different sectors to come together and adopt a whole system multi-agency approach to tackling and preventing serious violence at a local level, often referred to as a ‘public health approach’.

Then, in December 2019, the government announced that it would bring forward legislation to create a new Serious Violence Duty. This is expected to come into effect between 2022 and 2023 and will require responsible authorities to work together to prevent serious violence and create the conditions for information sharing between organisations to take effective coordinated action in their local areas.

To tackle violence the root causes of violence must be addressed; only focussing on enforcement is not enough. Violence of all sorts is strongly associated with social determinants and is a result of the interaction of several risk factors which span the individual, family, community and society.

No issue relating to violence has a single cause or a single solution; to have an impact on the various context and underlying risk factors that contribute to violence, different partners from across the system must work collaboratively and adopt a whole systems approach.[[2]](#footnote-2)

The [Prime Minister’s virtual summit on Hidden Harms](https://www.gov.uk/government/publications/prime-ministers-virtual-summit-on-hidden-harms) (June 2020) highlighted that all communities and every aspect of children’s and adult services have been affected by Covid-19, however experiences have varied, and for some this period will have been exceedingly difficult and traumatic.

National, regional and local systems are concerned about the increase to ‘hidden harms’. Crimes such as child abuse, child sexual exploitation, domestic abuse (including “honour”-based abuse), sexual violence and modern slavery, typically take place behind closed doors, hidden away from view.

[Building a country that works for all children post covid-19](https://adcs.org.uk/general-subject/article/pr-building-a-country-that-works-for-all-children-post-covid-19) (July 2020), highlights the vulnerabilities of specific cohorts, including children with additional health needs and disabilities, care leavers, young carers, families in conflict with the law and families with no recourse to public funds, which have been heightened during this period.

**South West regional response**

Following further discussion in region with our Public Health England Population Health & Wellbeing team a vision was agreed. We set out that there will be clear and consistent information governance arrangements in the management and future development of an effective system to prevent violence and to safeguard those at risk of harm and abuse across the South West region. it is anticipated that data shared will not include any personal identifiers with few exceptions as described in section 3 below.

Common understanding of information governance (IG) principles will be established across all organisations and underpinned by a high-level agreement across the South West region. This is that agreement. There may be a need to form a high-level advisory panel to facilitate cross organisational data sharing to improve the quality and efficiency of partnership data, including health and care services across the South West region.

In order to tackle serious violence in all its forms, we need to understand what good policing, health and social care looks and feels like to victims, survivors, perpetrators and offenders. This view needs to be based upon evidence rather than anecdote.

There will also be a resource containing exemplar material to support these activities. The practical tools and guidance associated with this agreement will be the start of that resource.

The issues this agreement seeks to address are:

* Processes for gathering IG advice can be complicated and often different answers are given by different organisations.
* Requests to share data are not enacted, despite there being a justification.
* Late consideration of IG advice.
* Complexity of the data and approvals landscape.
* Where to initiate a data sharing arrangement.
* Balancing low risk appetite/ being risk averse with finding creative solutions.

For initiatives involving multiple agencies, the above issues may need to be addressed by bringing together information governance professionals from partners in an Information Governance Advisory Panel (or equivalent) and establishing common understanding and application of IG principles through this agreement but being flexible enough to take account of varying organisational contexts. It would then be the remit of the Information Governance Advisory Panel to assess and report on progress and achievement.

# Aims of the framework

To provide the mechanism for establishing effective data sharing to support service led initiatives within the South West region and to be used, where beneficial, for any other data sharing across wider public services that include relevant data.

To simplify the establishment of data sharing arrangements across the South West region, by providing a common, consistent approach and template documentation to ensure relevant services work together to share data and knowledge and allow them to target interventions to prevent and tackle violence. Sharing initiatives established via this approach may engage organisations beyond the core South West region partners, such as universities and other partners where this is assessed as necessary and agreed by those entering into the initiatives.

# How the framework will work in practice:

This framework sets out an approach to support the sharing of data across two sharing paths:

* Sharing to safeguard those at risk of harm or abuse and;
* Sharing for the current management and future development of an effective system to prevent violence, described as ‘purposes other than safeguarding’.

These paths are described in more detail in sections 5 & 6.

At a strategic level, (national or regional) we do not expect that individual personal data will be routinely shared through the South West collaborative as, so far as practicable, local partnerships should have arrangements in place, which set out clearly the processes and the principles for sharing information and data internally. Local processes will outline how personal data can be shared through existing information gateways (for example, [multi-agency risk assessment conferences](https://safelives.org.uk/practice-support/resources-marac-meetings) (MARAC), [multi-agency public protection arrangements](https://www.gov.uk/government/publications/multi-agency-public-protection-arrangements-mappa--3) (MAPPA) and multi-agency safeguarding hubs (MASH) arrangements)[[3]](#footnote-3). However, there may be instances where information pertaining to individuals (including personal data) needs to be shared, a possible example if the police wish to discuss within or across boundaries a local gang and/or individuals’ patterns of behaviour that would be difficult to assess without partnership collaboration.

**Signing this agreement does not itself enable data sharing to be conducted. The requirements of the two paths above must be followed to establish operational data sharing.**

The appendices to this agreement identify the core legal powers and lawful bases for the sharing of data, so programmes, projects and other activities can assess and use these as required for the basis for their operational data sharing. **The appendices and support materials can be updated and developed without the need for partners to re-sign this agreement.**

The intent of this approach is to support initiatives in setting out data sharing arrangements. Where organisations do not require that support, i.e. they have their own template documentation, accessible expertise and are not encountering any difficulties in establishing arrangements, then this agreement is not mandatory.

The agreement will maintain and publish details of:

* Organisations invited to sign the agreement and those that have signed, noting their organisational status (i.e. public body, private organisation, voluntary sector and educational establishment) and whether they are a South West region partner or an associated organisation.
* The sharing initiatives utilising the agreement to provide their data sharing arrangements and links (where possible) to their operational documentation.

# Principles for sharing data

**Core principles:**

* The framework establishes the common bases and approach to sharing data for both the safeguarding of vulnerable individuals and other purposes.
* Sharing initiatives using the framework will build the specific detail required to reach agreement, using the approach, tools and reference material in the framework as required.
* Data sharing initiatives will be service led and driven by assessment of population need and potential to benefit.
* The South West collaboration is not a legal entity and therefore has no legal powers related to control of data. However, the South West collaboration has a responsibility to foster collaboration and communication between data controllers.
* Where a sharing initiative supported by the framework approach identifies organisations as joint controllers, specific arrangement documents will be established identifying how responsibilities are allocated. This will be based on an appropriate allocation for the initiative, not necessarily an equal split.
* Where an initiative is managed by joint controllers, whilst any of the joint controllers can receive a request from an individual in relation to their data protection rights, the ‘serious harm test’ related to an access request must be undertaken by the ‘appropriate professional’ in each contributing organisation in relation to the data that organisation has contributed (ref Data Protection Act 2018, Schedule 3, section 2). In the same manner determination of response to any request to erase, rectify, restrict or object to the use of data that has come from an individual organisational source must be considered by that organisation.
* The common law duty of confidentiality is met when:
* Organisations sharing data are reasonably sure that people have an expectation that their data will be shared.
* Data shared for a specific initiative has been ‘minimised’ to that which is deemed by an appropriate professional (i.e. health and care, Police or safeguarding staff) as necessary.
* Any new initiatives will employ anonymisation or pseudonymisation of data as early as possible to ensure they comply with the principle of ‘data minimisation’ under Article 5(1)(c) of UK GDPR.

The next two sections set out the principles that organisations signing this agreement will follow in any operational data sharing established under the remit of this agreement.

## Principles for safeguarding:

* Where provision of statutory services requires organisations to work together to safeguard an individual then use of personal data will be on the basis that *‘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’*[[4]](#footnote-4) as the basis for processing and not on the consent of the individual. ‘Discretionary’ services, where the individual may benefit from the service but does not ‘need’ the service, *may* require consent to share data.
* Organisations agreeing to share data are responsible for ensuring they are covered by the appropriate statutory bases on which any operational sharing is established and agreed (see appendix 3).
* For sharing initiatives supporting the safeguarding of individuals, the legal basis for use/sharing by care organisations is primarily:
* UK GDPR Article 6(1)e – ‘necessary for the performance of a task carried out in the public interest or in the exercise of official authority’[[5]](#footnote-5).
* UK GDPR Article 9(2)b – that the processing is necessary for the purposes of carrying out the obligations of the controller or data subject in the field of social protection law; the provisions of the Children Acts 1989 and 2004, and the Care Act 2014 are relevant, or
* UK GDPR Article 9(2)c – that the “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”, or
* UK GDPR Article 9(2)h – that the “processing is necessary for the purposes of … 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…”

Appendix 4 provides general guidance on the likely UK GDPR conditions in respect of different uses of data. However, this must be assessed on a case-by-case basis in consultation with information governance subject matter experts as there may be nuances that would cause uses to deviate from the ‘likely’ bases.

The data collected by the Police is processed for law enforcement purposes under Part 3 and an additional lawful basis needed to be identified to share under Part 2[[6]](#footnote-6).

# Principles for purposes other than safeguarding:

* Service providers can only use the data they hold in relation to managing and developing their own services. They can, by agreement, link with other providers to do this on a wider basis. They can also, by agreement, provide data to commissioning organisations to support the functions of those organisations.
* Commissioning organisations can only use data related to the population that they cover.
* Commissioning organisations can link their legal powers together across a wider geography (i.e. South West region or Integrated Care System) by establishing joint controller arrangements over combinations of data they wish to use.
* Providers can undertake data processing on datasets for commissioners by means of data processing agreements.
* Local authorities shall be seen as having both commissioner and provider functions in relation to the above statements.
* There will be an expectation that for any sharing other than for safeguarding this will be fully anonymised or de-personalised. Any potential sharing opportunity that includes Personal data will be assessed on a case-by-case basis.

**General Data Protection Regulation - justifications and common law of confidentiality applied to core ‘non safeguarding purposes’ (NB this list is a non-exhaustive list of examples)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Purposes** | **GDPR Article 6** | **GDPR Article 9** | **Common law of confidentiality** |
| **Risk stratification for service planning** | Necessary for the performance of a task carried out in the public interest or in the exercise of official authority. | Management of health or social care systems and services on the basis of member state law | Requires linkage between data sources, via pseudonymised data either at source or via controlled environment where data processing is automated and not conducted manually by users. |
| **Managing finances, quality & outcomes** |
| **Planning, implementing and evaluating population health strategy** |
| **Undertaking research** | Necessary for the performance of a task carried out in the public interest or in the exercise of official authority. **(Public Authority)**  Legitimate interests **(Private organisation)** | necessary for … scientific research purposes or statistical purposes in accordance with Article 89 (1) based on member state law (see legal gateways) 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 rights and interests of the data subject. | Requires linkage between data sources, via pseudonymised data either at source or via controlled environment where data processing is automated and not conducted manually by users. |

* National data opt out: All sharing initiatives under this approach will consider and where applicable link to the National Data Opt Out (NDOO) where it involves the use of health or care data. The application of the NDOO will be considered both at the organisational level before data is shared and in any shared analytics/intelligence platform. Its application will be confirmed in the DPIA for a specific initiative.

# Process for establishing initiative specific data sharing arrangements

Each data sharing initiative (or an existing initiative at the point of review) within the scope of, or requiring the support of this agreement will:

* Set out the service led uses and purposes for data sharing.
* Demonstrate how it will consider engagement with stakeholders and inclusively undertake any engagement identified as necessary. This to include the public, both from the perspective of concerns around the use of their personal data and the benefits/impacts and justifications for undertaking the initiative in general.
* Set out the best approach to enable the data sharing, based on the principles, processes and reference materials in this agreement.
* From the identified purposes for sharing, detail the relevant legal gateways and lawful basis, drawing on the detail and approach set out in this agreement and applying them as relevant to the sharing initiative.
* Confirm the status of the organisations involved (i.e. controller, processor etc) and where required, establish joint controller arrangements.
* Identify the data types/items, the method of exchange, the risks and agreed mitigation controls, including pseudonymisation and encryption of data as required by DPIA.
* Conduct a data protection impact assessment (DPIA) that is compliant with ICO guidance on conducting DPIAs. A template form is available but use of this form is not mandatory.
* Where agreed between the parties, in line with ICO guidance an operational data sharing agreement can be established.
* Each controller involved in an initiative will need to maintain ‘records of processing activities’ in line with data protection legislation, which may include data flow maps, access control matrices and associated documents. **Where possible the initiative will develop these once and share**.

The aim of the practical implementation of the agreement (and associated templates) is to ensure all initiatives supported have clear and consistent documentation on sharing, minimising any duplication and utilising any related documentation that the initiative needs on an operational basis (i.e. a shared care record will have a role based access matrix as part of project documentation).

**Step through process:**

* Identify stakeholders involved & service led drivers for the data sharing
* Identify lead for DPIA
* Conduct DPIA, involving consultation with stakeholders and public as required
* Where potential joint controllers identified, assess and where required set out joint controller arrangement
* The DPIA will go to the IG leads of each affected Controller (which may form an Information Governance Advisory Panel) on the following basis:
  + Initial awareness
  + For advice on any specific issues/risks identified where a wider selection of views and analysis will help resolve issues
  + Confirmation of agreement to DPIA by relevant partners (an Information Governance Advisory Panel would not be an ‘approving body’)
* Report on risk mitigation in DPIA (i.e. what’s in place, what’s being established)
* All stakeholders to review and approve DPIA via internal organisational process
* Sharing initiated either by agreement to Operational DSA (as required) or by enablement of service/provision of data

# Organisational commitments

All parties signing the South West Regional Serious Violence and Contextualised Safeguarding IG framework commit to:

* Share relevant data for specific sharing initiatives, with any other relevant agency involved in the sharing initiative, where the process for establishing specific sharing arrangements has been conducted and the detail of the sharing has been agreed by all relevant parties. Any agreement established will not prevent any party withdrawing their participation from a sharing initiative.
* Where they participate in a sharing initiative, to inform data subjects about the sharing of data related to the safeguarding of individuals and the use of data for purposes other than safeguarding, noting that sharing is not restricted by organisational and geographical boundaries and that relevant information will be shared where necessary.
* Where data is shared via a shared system, then the relevant partners will maintain ‘records of processing’ in line with data protection legislation, including identifying which data is shared and how any access control will be implemented.

# Sharing partner assurances

Through the completion of a DPIA for any new use of data, it should be considered whether sharing partners must meet standards that qualifies them to partake in a data sharing initiative. An example of a required qualifying standard is provided in Appendix 5.

***Sign up to this framework does not indicate that an organisation meets any qualifying standard***.

# Appendix 1. Tools to support sharing initiatives

**Data Protection Impact Assessment (DPIA) template:**

Use of this template is not mandatory, provided the sharing initiative completes a DPIA that is compliant with the ICO guidance on completing DPIAs.

* Describe the nature, scope, context and purposes of the processing;
* Assess necessity, proportionality and compliance measures;
* Consider and undertake any stakeholder and public consultation
* Confirm the legal gateways, the lawful basis for sharing and the implications of any specific legislation or regulation on the context of the sharing across all relevant partners.
* Identify and assess risks to individuals; and identify any measures to mitigate those risks.
* Identification of all controllers and description of their status, i.e. individual, joint etc..
* Identification of all processors and relevant contractual agreements – noting where these are required and assessing that they are put in place
* Process for the controller’s subject to the DPIA to agree the risks identified, the mitigation controls and the process for auditing sufficiency during the sharing programme.
* Mitigation controls will include:
  + Technical measures, operating processes, common standards/accreditations, agreed data flow maps/records of processing activities & access controls (i.e. Role Based Access Controls) and associated processes



**Operational Data Sharing Agreement Template**

The template available here can be used where a sharing initiative has identified the need for a specific operational document setting out the detail of the sharing, including the data items, method and other specifics, where documented agreement is required between partners.



**Joint Controllership Assessment & Arrangements Template**

Where a DPIA for a sharing initiative has identified that some controllers are acting in a joint controllership capacity, the template below can be used to assess whether the controller are joint and if so to set out the arrangements required by GDPR Article 26.



**File sharing / collaboration platform**

It is recommended that, for any initiative involving multiple stakeholders, a file-sharing/collaboration platform is used to improve accessibility, avoid duplication and manage version control effectively.

# Appendix 2. Reference materials: the components of data sharing.

Data sharing between agencies requires the following to be in place:

* Identified roles and responsibilities of the organisations sharing data.
  + Organisations which determine the purposes and means for sharing personal data are ‘controllers’ of that data. This can be separately or on a joint basis.
  + Organisations that undertake processing of data but do not determine the purposes and means and act only on instructions of a controller are processors.
* Legal powers (a.k.a ‘legal gateways’) – legislation that gives public bodies their legal powers to provide services. It is implicit within many such services that data is recorded and shared to ensure those services can be provided across agencies. These powers can be delegated by service contract to a private organisation. Private organisations do not need legislation establishing their functions/activities in the same way, but must ensure all their activities are lawful.
* Lawful basis – personal data and special category personal data cannot be used unless the purpose is covered by justifications for using personal data in data protection legislation. Data Protection principles also require that any other relevant laws related to the data processing are identified and complied with.
* Application of data protection legislation principles to the data sharing, including:
  + Agreed basis on how data sharing partners can demonstrate their accountability in relation to the data sharing.
  + Where any sharing is under joint controllership then there needs to be an agreed arrangement to how data subject rights are managed.
  + Agreed approach to the management of incidents and breaches where data shared is jointly controlled. Reliant on individual organisational policy in other circumstances.

**Legal Powers to share data (legal gateways)**

Under this agreement, information sharing is defined as two distinct paths:

1. Sharing of data for the safeguarding of an individual. This includes the use of analysis tools on data that can provide useful ‘intelligence’ to the safeguarding professional(s) determining the best action to safeguard an individual.
2. Use for purposes other than safeguarding an individual, which do not directly benefit/impact the individual, such as service evaluation, redesign, research and development of methods to prevent violence.

Reference material and links to the legal gateways to share data for each path are to be found in Appendix 3.

**Lawful bases to process data**

The requirement for lawful basis comes from the need to comply with relevant sections of the UK General Data Protection Regulation, the Data Protection Act 2018 and any other relevant law, including the common law of confidentiality.

The relevant lawful basis elements for each path are set out in sections 5 & 6.

**Application of data protection principles to each ‘path’**

The following table sets out key requirements related to each ‘path’ that are the starting points for a sharing initiative to set out. This is to support the DPIA that the initiative needs to conduct and promote a consistent baseline.

|  |  |  |
| --- | --- | --- |
| **Principle** | **Path 1 – Safeguarding** | **Path 2 – Purposes other than safeguarding** |
| Processed lawfully, fairly and in a transparent manner | See section 5 | See section 6 |
| Processed for specific purposes and not further processed in a manner that is incompatible | Satisfied if purpose is to safeguard an individual | Partners should specify that data is used for these purposes in their ‘fair processing’ notices. GDPR Article 5(1)b also highlights that research and statistical purposes compliant with Article 89 are not incompatible. This will be assessed by relevant DPIA(s). |
| Adequate, relevant and limited to what is necessary | Application of controls such as role based access, legitimate relationships (in shared systems) and justification for the inclusion of data items | Application of controls such as role based access, legitimate relationships (in shared systems) and justification for the inclusion of data items. Specific consideration of items related to the identity. Anonymisation or pseudonymisation being applied as early as possible |
| Accurate and where necessary kept up to date | Individual controller responsibility leading to potential joint responsibility in shared record systems and processes supporting safeguarding | Dependent on application of the principle to data sources used for safeguarding. Processes to extract and combine data need to consider checks to ensure processing does not compromise quality |
| Kept in a form that permits identification for no longer than is necessary | Application of retention periods already defined in contributing sectors. May need specific consideration of variation between sectors in combined shared records | Application of already defined retention periods. In addition data that has been pseudonymised may be retained for longer (where assessed as compliant with Article 89 of GDPR). |
| Processed in a manner that ensures appropriate security | Assessed via DPIA for programme and identification of appropriate controls | Assessed via DPIA for programme and identification of appropriate controls |

# Appendix 3. Reference materials: Legal gateways supporting data sharing

**Legal gateways supporting purposes other than the safeguarding of an individual.**

These can be accessed via the NHS England Secondary Use Data Governance Tool (<https://data.england.nhs.uk/sudgt/>). A list of purposes other than safeguarding is available at: <https://data.england.nhs.uk/sudgt/activities> and by clicking through each purpose the detail of the legal gateways and the organisations they are applicable to can be accessed.

**Legal gateways supporting the safeguarding of an individual (not an exhaustive list)**

| **Legislation** | **Legal gateway** | **Organisation** |
| --- | --- | --- |
| Health and Social Care (Quality & Safety) Act 2015 | Section 3 (1),(2)(a)(b):   1. This section applies in relation to information about an individual that is held by a relevant health or adult social care commissioner or provider (“the relevant person”). 2. The relevant person must ensure that the information is disclosed to (a)persons working for the relevant person, and (b)any other relevant health or adult social care commissioner or provider with whom the relevant person communicates about the individual. | All commissioners and providers of health and care services to Adults. |
| Health & Social Care Act 2012 | Section 195:  (contains guidance about) specific duties of co-operation, including creating a Health and Wellbeing Board, which must, for the purpose of advancing the health and wellbeing of the people in its area, encourage persons who arrange for the provision of any health or social care services in that area to work in an integrated manner. | All commissioners and providers of health and care services. |
| Care Act 2014 | Section 1:  The general duty of a local authority, in exercising a function under this Part in the case of an individual, is to promote that individual’s well-being.  Well-being in this Part includes:  (b) physical and mental health and emotional well-being;  (c) protection from abuse and neglect;  (f) social and economic well-being; | Local authorities as commissioners and providers of health and care services to adults, and those commissioned to provide those services. |
| Care Act 2014 | Section 3:  Local authorities must exercise their functions under this Part with a view to ensuring the integration of care and support provision with health provision and health-related provision where it considers that this would —  (a) promote the well-being of adults in its area with needs for care and support and the well-being of carers in its area,  (b) contribute to the prevention or delay of the development by adults in its area of needs for care and support or the development by carers in its area of needs for support, or  (c) improve the quality of care and support for adults, and of support for carers, provided in its area (including the outcomes that are achieved from such provision). | Local authorities as commissioners and providers of health and care services to adults, and those commissioned to provide those services. |
| Care Act 2014 | Section 42: Enquiry by local authority**E+W**  This section has no associated Explanatory Notes   1. This section applies where a local authority has reasonable cause to suspect that an adult in its area (whether or not ordinarily resident there)—   (a) has needs for care and support (whether or not the authority is meeting any of those needs),  (b) is experiencing, or is at risk of, abuse or neglect, and  (c) as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.   1. The local authority must make (or cause to be made) whatever enquiries it thinks necessary to enable it to decide whether any action should be taken in the adult's case (whether under this Part or otherwise) and, if so, what and by whom. | Local authorities as commissioners and providers of health and care services to adults, and those commissioned to provide those services. |
| The Children Act 1989 | Section 47(9)(11):  Where a local authority are conducting enquiries under this section, it shall be the duty of any person mentioned in subsection (11) to assist them with those enquiries (in particular by providing relevant information and advice). The persons are—  (a) any local authority;  (d) any clinical commissioning group, Local Health Board , Special Health Authority, National Health Service trust or NHS foundation trust; and  (e) any person authorised by the Secretary of State for the purposes of this section. | Local Authorities conducting child protection enquiries and those that have a duty to assist (health bodies). |
| The Children Act 1989 | A local authority may also request help from those listed above in connection with its functions under Part 3 of the Act. Part 3 of the Act, which comprises of Sections 17-30:  (allows for local authorities to provide various types of support for children and families).  Section 17(5):  Every local authority—  (a) shall facilitate the provision by others (including in particular voluntary organisations) of services which it is a function of the authority to provide by virtue of this section, or section 18, 20, 22A to 22C, 23B to 23D, 24A or 24B**]**; and  (b) may make such arrangements as they see fit for any person to act on their behalf in the provision of any such service. | Local Authorities facilitating services to those identified as “in need” and those that are commissioned to provide the  service. |
| The Children Act 2004 | Section 10:  Co-operation to improve well-being.   1. The arrangements are to be made with a view to improving the well-being of children in the local authority’s area so far as relating to—   (a) physical and mental health and emotional well-being;  (b) protection from harm and neglect; (e) Social and economic well-being.   1. for the purposes of this section each of the following is a relevant partner:  * District councils * The police * The probation service * Youth offending teams (YOTs) * Health and Wellbeing Board. * Any clinical commissioning group for an area any part of which falls within the area of the authority | Local Authorities and relevant partners that have the remit to improve the well-being of children. |
| The Children Act 2004 | Section 11:  Arrangements to safeguard and promote welfare.  The section applies to:  (a) a local authority in England;  (b) a district council which is not such an authority;  (bb) a clinical commissioning group;  (d) a Special Health Authority, so far as exercising functions in relation to England, designated by order made by the Secretary of State for the purposes of this section;  (f) an NHS trust all or most of whose hospitals, establishments and facilities are situated in England;  (g) an NHS foundation trust;  (h) the local policing body and chief officer of police for a police area in England;  (k) a youth offending team for an area in England;  (l) the governor of a prison or secure training centre in England (or, in the case of a contracted out prison or secure training centre, its director); | Local Authorities and relevant partners that have a duty to safeguard and promote welfare of children. |
| Childcare Act 2006 | Section 1:  General duties of local authority in relation to well-being of young children   1. an English local authority must—   (a) improve the well-being of young children in their area, and  (2) in this Act “well-being”, in relation to children, means their well-being so far as relating to—  (a) physical and mental health and emotional well-being;  (b) protection from harm and neglect;  (e) social and economic well-being. | Local authorities as commissioners and providers of health and care and services to children, and those commissioned to provide those services. |
| Childcare Act 2006 | Section 4:  Duty of local authority and relevant partners to work together**E+W**   1. This section has no associated Explanatory Notes 2. For the purposes of this section each of the following is a relevant partner of an English local authority—   (za) the “National Health Service Commissioning Board;”, and  (a) a clinical commissioning group for an area any part of which falls within the area of the local authority;  (b) the Secretary of State, in relation to his functions under section 2 of the Employment and Training Act 1973 (c. 50). | Local authorities as commissioners and providers of health and care and services to children, and those commissioned to provide those services. |
| Children and Families Act 2014 | Section 23:  Places a duty on health bodies (CCGs, NHS Trust and NHS foundation trust) to bring certain children to local authority’s attention, where the health body has formed the opinion that the child has (or probably has) special educational needs or a disability. | Health bodies and local authorities. |
| Children and Families Act 2014 | Section 25:  Places a duty on a local authority to exercise its functions with a view to ensuring the integration of educational provision, training provision with health care and social care provision where it thinks that this would –  (a) promote the well-being of children or young people in its area who have special education needs or a disability, or  (b) improve the quality of special educational provision in its area or outside its area for children it is responsible for who have special educational needs | Local authorities as commissioners and providers of health and care and services to children, and those commissioned to provide those services. |
| Crime and Disorder Act 1998 | Section 17:  Duty to consider crime and disorder implications.   1. Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in its area. 2. This section applies to a local authority, a joint authority, a local policing body, and others. | Local authorities and the Police |
| Digital Economy Act 2017 | Section 35 (1)(2)(9)(10)(11)(12):  Disclosure of information to improve public service delivery.  This section has no associated Explanatory Notes   1. A specified person may disclose information held by the person in connection with any of the person’s functions to another specified person for the purposes of an objective which is a specified objective in relation to each of those persons. 2. In this section “specified person” means a person specified, or of a description specified, in Schedule 4   (9) The first condition is that the objective has as its purpose—  (a) the improvement or targeting of a public service provided to individuals or households, or  (b) the facilitation of the provision of a benefit (whether or not financial) to individuals or households.  (10) The second condition is that the objective has as its purpose the improvement of the well-being of individuals or households.  (11) The reference in subsection [(10)](http://www.legislation.gov.uk/ukpga/2017/30/section/35/enacted#section-35-10) to the well-being of individuals or households includes—  (a) their physical and mental health and emotional well-being,  (b) the contribution made by them to society, and  (c) their social and economic well-being.  (12)The third condition is that the objective has as its purpose the supporting of—  (a) the delivery of a specified person’s functions, or  (b) the administration, monitoring or enforcement of a specified person’s functions. | Local authorities as commissioners and providers of health and care and services, and those commissioned to provide those services. |
| Local Government Act 2000 | Section 2  Promotion of well-being.**E+W**   1. This section has no associated Explanatory Notes 2. Every local authority are to have power to do anything which they consider is likely to achieve any one or more of the following objects—   (b) the promotion or improvement of the social well-being of their area, and | Local Authorities |
| National Health Service Act 1977 | Section 22:  Co-operation between health authorities and local authorities.**E+W+S**   1. In exercising their respective functions NHS bodies (on the one hand) and local authorities (on the other) shall co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.   In this section “NHS body” means—  (za) a Strategic Health Authority;  (a) a Health Authority;  (b) a Special Health Authority;  (d) an NHS trust.**]** | Health bodies and local authorities. |
| National Health Service Act 2006 | Section 82:  Places a duty on NHS bodies and local authorities to co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales. | Health bodies and local authorities as commissioners and providers of health and care and services, and those commissioned to provide those services. |
| Special Education Needs and Disability Regulations 2014 | Section 6:  Where the local authority secures an EHC needs assessment for a child or young person, it must seek the following advice and information, on the needs of the child or young person, and what provision may be required to meet such needs and the outcomes that are intended to be achieved by the child or young person receiving that provision—  (c) medical advice and information from a health care professional identified by the responsible commissioning body;  (d) psychological advice and information from an educational psychologist;  (e) advice and information in relation to social care;  (f)advice and information from any other person the local authority thinks is appropriate;  (h) advice and information from any person the child’s parent or young person reasonably requests that the local authority seek advice from. | Local authorities as commissioners and providers of health and care and services to children, and those commissioned to provide those services. |

# Appendix 4. Application of UK GDPR Article 6 and 9 processing conditions to uses of data for purposes related to reducing serious violence and safeguarding concerns

| **UK GDPR Article 6 or Article 9 processing condition** | **Data uses, related to reducing serious violence and safeguarding concerns, likely to fall under processing condition** |
| --- | --- |
| Art 6(1)a “the data subject has given consent to the processing of his or her personal data for one or more specific purposes” | This could apply to uses of data on victims or witnesses, unless overruled by public interest or a legal duty, which would be covered by another processing condition. |
| Art 6(1)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” | Unlikely to apply, unless data used is part of service provided to the data subject (e.g. a private health service and the use of data was included in the agreement/contract between service provider and data subject). |
| Art 6(1)c “processing is necessary for compliance with a legal obligation to which the controller is subject” | Likely to apply where data is being used/shared for a purpose for which the Controller has a duty, power or is required, in law, to use/share the data for. |
| Art 6(1)d “processing is necessary in order to protect the vital interests of the data subject or of another natural person” | Likely to apply where data is used/shared in an emergency situation, to protect an individual from immediate serious harm or death. |
| Art 6(1)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” | Likely to apply where data is used for a purpose/task, for which the majority of the general public would expect the data to be used, or where the data is used by an organisation in respect of fulfilling a statutory function. |
| Art 6(1)f “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party…” | Unlikely to be applicable in this context. However, if 6(1)c nor 6(1)e applies, then this could be considered. |
| Art 9(2)a “the data subject has given explicit consent to the processing…” | This could apply to uses of data on victims or witnesses, unless overruled by public interest or a legal duty, which would be covered by another processing condition. |
| Art 9(2)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 insofar as it is authorised by domestic law…” | Likely to link to key parts of social protection law, giving controllers a duty or power (depending on applicable law) to use/share relevant data for tackling serious violence and safeguarding concerns. |
| Art 9(2)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” | Likely to apply where data is used/shared in an emergency situation, to protect an individual from immediate serious harm or death. |
| Art 9(2)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…” | Unlikely to apply, unless data used relates to a member of such a body – the processing condition does not apply to any disclosures outside of the body. |
| Art 9(2)e “processing relates to personal data which are manifestly made public by the data subject” | Unlikely to apply, as likely, even if such data was used, that another, more appropriate processing condition would apply. |
| Art 9(2)f “processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity” | Possible this would apply, as data used could become relevant a legal claim. |
| Art 9(2)g “processing is necessary for reasons of substantial public interest…” | This is likely to apply in many circumstances where organisations are subject to legal duties, powers etc, to use/share data to tackle serious violence and safeguarding concerns[[7]](#footnote-7). |
| Art 9(2)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…” | Likely to apply where use of data relates to the provision or management of health or social care services. |
| Art 9(2)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…” | Unlikely to apply to uses of data for tackling serious violence and safeguarding concerns. It has a relation to public health, but this condition lends itself more specifically to processing of data necessary to tackle serious cross border threats (such as a pandemic), etc |
| Art 9(2)j “processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…” | Unlikely to apply until such time as there is no longer necessity to retain data under other processing conditions and so data may be appraised and retained for longer should this condition apply. |

# Appendix 5. Qualifying Standard (Example)

The Qualifying Standard for organisations to achieve to sign up to this sharing agreement is achievement of ‘standards met’ to the current version of the Data Security & Protection Toolkit (<https://www.dsptoolkit.nhs.uk/>).

**Where organisations have completed the toolkit but not achieved ‘standards met’.**

In these cases, organisations will be asked to:

* Confirm the standards within DSP Toolkit that they have not met
* Confirm the timescale by when they plan to achieve these standards
* Identify any other standards/accreditations they have that relate

The Information Governance Advisory Panel (or equivalent) will receive and consider the position of the organisation and make recommendation to systems’ Digital Strategy Group (or equivalent) that the organisation can/cannot sign at this time.

**Where organisations are not required to complete the DSP Toolkit**

Organisations in this position will be invited to complete the DSP Toolkit voluntarily. If they are unwilling to do so, perhaps on the basis that they have already achieved other accreditations related to information governance and data security then the Information Governance Advisory Panel (or equivalent) will invite them to detail those accreditations along with any narrative the organisation wishes to provide. This will be reviewed by the panel and any recommendation made provided to the Digital Strategy Group (or equivalent) for consideration.

**Where an organisation has previously been compliant with DSP Toolkit or other approved accreditation but it has expired.**

The organisation will be asked to confirm their plans for reviewing and updating their DSP Toolkit or accreditation. The Information Governance Advisory Panel (or equivalent) will make recommendations to the Digital Strategy Group (or equivalent) having considered the organisation’s submission.

# Appendix 6. Signature of agreement to framework

|  |  |
| --- | --- |
| **Signed on behalf of (Insert org name)** | |
| **Name** |  |
| **Job title** | *This may be the organisation’s Senior Information Risk Owner, Caldicott Guardian or a representative with equivalent authority* |
| **Signature** |  |
| **Date** |  |

Alternatively, an email confirming sign up to the framework from the signatory will be accepted.

1. HM Government, A whole-system multi-agency approach to serious violence prevention, (2019), page 21. [↑](#footnote-ref-1)
2. As above. [↑](#footnote-ref-2)
3. Other examples of guidance see [Working together to safeguard children (2018)](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2) has recently updated the Information Sharing section on 9th December 2020, pages 18-22, para 24-28. [↑](#footnote-ref-3)
4. The ‘official authority’ is established in the legislation that gives an organisation the duty or power to perform the function for which the processing of personal data is deemed necessary. [↑](#footnote-ref-4)
5. as above. [↑](#footnote-ref-5)
6. The legal basis for use/sharing by the Police is primarily in accordance with section 35 and the processing conditions set out in schedule 8 of the UK Data Protection Act 2018 and relevant additions (by way of Secretary of State regulations). [↑](#footnote-ref-6)
7. For further information refer to [What are the substantial public interest conditions? | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/) [↑](#footnote-ref-7)