



## **Tier 2-Preventing Crime & Disorder Information and Data Sharing Agreement**

**For multi-agency partnership working together to:  
Reduce the levels and impact of Crime and Anti-Social Behaviour on communities across Bristol**

A specific information sharing agreement which is guided by, and should be used in conjunction with, the overarching Tier 1- Keeping Bristol Safe Partnership's Safeguarding and Community Safety Information and Data Sharing Agreement.

# Contents

---

## Introduction

### Anti-Social Behaviour Data Sharing Agreement

- 1 Administration
- 2 Purpose and benefits
- 3 Data Controller(s) / Joint Controller(s)
- 4 Processor(s)
- 5 Data shared between partners.
- 6 Lawfulness – UK GDPR lawful basis and Article 9 condition
- 6A Lawfulness – Data Protection Act 2018
- 6B Lawfulness – legal powers and gateways
- 7 Non-interference – Common law duty of confidentiality
- 7A Non-interference – Human Rights Act 1998, Article 8
- 8 Transparency
- 9 Individual's rights
- 10 How data sharing will be carried out
- 11 Processing outside of the UK
- 12 Accuracy of data before sharing
- 13 Rectification of data that has been shared
- 14 Retention and disposal
- 15 Breach management
- 16 IG contacts
- 17 Review
- 18 Variation
- 19 Ending the agreement.
- 20 End date

**21 Signatories**

**22 Abbreviations and glossary**

# **Preventing Crime & Disorder Information & Data Sharing Agreement (DSA)**

---

**Keeping Communities Safe Partnership**

between

**Signatories of this Agreement**

# 1 Administration

The organisations below are signatories to this Data Sharing Agreement:

Organisation	Address	ICO registration number	Contact person	Contact details
Bristol City Council	City Hall, College Green, Bristol, BS1 5TR	Z5873747	Ben Hewkin DPO	<a href="mailto:Data.protection@bristol.gov.uk">Data.protection@bristol.gov.uk</a>
Avon and Somerset Constabulary	PO Box 37, Valley Road, Portishead, Bristol, BS20 8QJ	Z4882079	Kevin Coe – Information Governance Manager	<a href="mailto:DPO@avonandsomerset.police.uk">DPO@avonandsomerset.police.uk</a>
Avon Fire and Rescue Service	Police & Fire Headquarters PO Box 37 Valley Road Portishead Bristol BS20 8JJ	Z6748396	Caldicott Guardian	<a href="mailto:DPO@avonfire.gov.uk">DPO@avonfire.gov.uk</a> <a href="mailto:foi-dp@avonfire.gov.uk">foi-dp@avonfire.gov.uk</a>
Bristol, North Somerset and South Gloucestershire Integrated Care Board (BNSSG ICB)	100 Temple Street, Redcliffe, Bristol BS1 6AG	ZB344972	DPO	<a href="mailto:bnssg.foi@nhs.net">bnssg.foi@nhs.net</a>
Ministry of Justice- Includes:	102 Petty France London SW1H 9AJ	Z5679958	DPO	<a href="mailto:dpo@justice.gov.uk">dpo@justice.gov.uk</a>

## Tier 2-Preventing Crime & Disorder Information and Data Sharing Agreement

HM Prison & Probation Service, Courts and Tribunal Judiciary				
--	--	--	--	--

The Keeping Bristol Safe Partnership Business Unit manages the full list of signatories to this agreement.

**General:**

---

<b>Date DSA comes into force:</b>	20/12/2024
<b>Last review:</b>	
<b>Date for review of DSA:</b>	20/12/2025 (12 months from last review)
<b>DSA Owner (Organisation):</b>	Bristol City Council
<b>DSA Author(s):</b>	Richard Hawkridge/Kevin Coe

**Version control:**

Version	Date	Author	Edit/Update
VO_1	27/06/2024	J.Howarth/R.Hawkridge/N.Ramjane	First draft
	08/2024	Kevin Coe/Richard Hawkridge	Change to statutory instruments, addition of scenarios, GDPR section
	02/09/24	Lynne Miller/Natasha Casling/Richard Hawkridge	Incorporation of BCC IG (LM and NC) comments into document.
	03/09/24	Richard Hawkridge/Joanna Warren	Avon Fire and Rescue (Joanna Warren) comments incorporated.
	13/09/24	Richard Hawkridge/Lucy Hunt/Natasha Casling	BNSSG (LH) comments incorporated and BCC IG (NC) further comments incorporated.
VO_2	17/09/24	Lizzie Lambrou	Proofreading edits
VO_3	16/10/24	Lizzie Lambrou	Finalising of document ready for signatures by statutory partners
	11/12/24	Lizzie Lambrou	Details to sections 8, 12, 13, 14, 15, 16
	13/12/2024	Lizzie Lambrou	Appendix A added



## 2 Purpose and benefits

---

### Overview:

The Keeping Communities Safe Board is a multi-agency group accountable to the Keeping Bristol Safe Partnership (KBSP) Executive Board (the Executive). The purpose of the group is to drive the delivery of the Executive's Strategic and Business Plan in relation, but not limited to, the duties and responsibilities as defined by the Crime and Disorder Act (1998), Crime & Disorder Formation & Implementation of Strategies Regulations 2007 and subsequent legislation pertaining to community safety, crime and disorder, and anti-social behaviour (ASB). In summary terms, the purpose that is relevant here is the reduction of Crime and Disorder.

### Purpose(s) and benefits for sharing information:

Sharing the right information, at the right time, with the right people is fundamental to good practice in safeguarding communities through the prevention of Crime and Disorder (including ASB). The Crime and Disorder Act 1998 is a piece of legislation that seeks to prevent such behaviour. Section 115 of the Act provides the lawful power for anyone to disclose information to a relevant authority – the police, police authority, local authority, Fire and Rescue, Probation, or health authority, or to any persons acting on their behalf – where this is necessary or expedient for the purposes of a provision of the Act i.e. for the prevention of Crime and Disorder (including ASB). This agreement is written with the intention of enabling and facilitating information sharing between those agencies (and those bodies acting on their behalf) to prevent Crime, Disorder and ASB in line with their duties as set out in Section 17 of the Crime and Disorder Act 1998.

By agreeing to this Information and Data Sharing Agreement, agencies will ensure that their single agency information sharing arrangements comply with the principles contained herein and enable such information sharing to occur at strategic, tactical, and operational levels. In doing so, parties to this agreement acknowledge that this does not interfere with their individual agency's responsibilities within the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR) because the information to be disclosed will fall within the exemptions allowed by that Act and those regulations as well as being in line with the legislation mentioned above.

This guidance therefore covers information sharing (both non-personal, personal, and sensitive) in a range of contexts relating to Community Safety including:

- Raising concerns and making referrals about situations in which Crime and Disorder is occurring and/or needs prevention.
- Undertaking and sharing the outcomes of learning from case reviews.
- Responsibilities to share information and make referrals to DBS and/or professional bodies.
- Information exchange, in the context of allegation management, between the relevant managers in the relevant services.
- Information exchange between the personnel working for and on behalf of the statutory community safety partners (and those bodies acting on their behalf) to prevent Crime, Disorder and ASB.
- Sharing qualitative and quantitative data to inform the work of the Keeping Communities Safe Board (the crime reduction partnership) and its various sub-boards.

Some examples of when such information sharing may take place include (but are not limited to):

- Sharing of pseudonymised data sets to allow geographic hotspot and repeat victim/perpetrator identification on case-by-case basis.
- Sharing of information relating to individuals with suspected mental illness who are causing alarm, harassment, and distress to other members of their community.
- Sharing of information regarding ownership and management of a premise where there is suspected Modern Slavery/exploitation occurring.
- Sharing of information about adults and children in a situation where it is suspected there is some criminal or sexual exploitation.
- Sharing of information relating to an individual's drug and alcohol treatment where such treatment plays a role in preventing that individual from causing crime and disorder.
- Sharing of information in multi-agency fora to inform problem solving discussions e.g. MARAC, ASB Multi-Agency Meetings, ASB Case Conferences, Hate Crime Operational Group, Modern Slavery Operational Group, Channel etc.
- Sharing of information about individuals involved in serious violence.

### 3 Data Controller(s) / Joint Controller(s)

**Please add all organisations which are controllers and are party to this Sharing Arrangement.**

Please provide specific details in the 'Status' column about the organisations' involvement as a Controller, such as 'contributing data as a controller', 'viewing data only as a controller', 'performing the following processing functions: <list>' and 'determined the purposes and means of processing for <activity> jointly with (if applicable) <name organisation>'.

Name of Organisation(s):	Status:
Bristol City Council – Relevant Authority	Local authority (BCC)-contributing data as a controller, viewing data, performing the following processing functions; confirming name, address, DOB, behaviour which is being discussed, history involving the named individual which pertains to the behaviour being discussed.
Avon & Somerset Police – Relevant Authority	Police-contributing data as a controller, viewing data, performing the following processing functions; confirming name, address, DOB, behaviour which is being discussed, history involving the named individual which pertains to the behaviour being discussed.
Avon Fire & Rescue – Relevant Authority	AF&RS-contributing data as a controller, viewing data, performing the following processing functions; confirming name, address, DOB, behaviour which is being discussed, history involving the named individual which pertains to the behaviour being discussed.
Bristol North & South Gloucestershire Integrated Care Board (BNSSG ICB) - Relevant Authority	BNSSG ICB-contributing data as a controller, viewing data, performing the following processing functions; confirming name, address, Date Of Birth (DOB), behaviour which is being discussed, history involving the named individual which pertains to the behaviour being discussed.

Ministry of Justice- Includes:  
HM Prison & Probation Service ,  
Courts and Tribunal Judiciary – Relevant Authority

MoJ-contributing data as a controller, viewing data, performing the following processing functions; confirming name, address, DOB, behaviour which is being discussed, history involving the named individual which pertains to the behaviour being discussed.

## Joint Controller responsibilities

Where organisations are joint controllers, they have shared responsibilities for complying with data protection laws, however they must agree how to attribute obligations between them in compliance with Article 26 of the UK GDPR. This template is set out to determine the obligations attributed to each joint controller (this may need to be completed more than once if there is more than one joint controller arrangement). This would be completed with assistance from Data Protection Officer(s). If the sharing includes some controllers who are not joint, then their compliance requirements are set out throughout the DSA (single controller responsibilities, if no joint controller arrangement, are also set out throughout the DSA).

Area of responsibility:	Joint Controller A:	Joint Controller B:	Joint Controller C:
<b>Conduct DPIA on the data processing.</b>	n/a		
<b>Individuals are informed about the use of their data (unless an exemption applies): Develop privacy information.</b>			
<b>Data is processed lawfully: Define the shared purposes for use of the data via this agreement.</b>			
<b>Data is used for limited purposes: Establish agreed purposes and if necessary, a process to identify, assess and agree other uses with the controllers.</b>			

Area of responsibility:	Joint Controller A:	Joint Controller B:	Joint Controller C:
<p><b>The minimum data is used: Ensure the minimum necessary data is used by staff.</b></p>			
<p><b>Data is accurate: Ensure processes to link and/or display data do not compromise accuracy.</b></p>			
<p><b>Data retained only as long as necessary: Ensure data is not kept for longer than appropriate periods.</b></p>			
<p><b>Define and implement appropriate security controls for the relevant exchange of data. Where a system is used - security control definition: Identify risks and design appropriate control measures to secure the system.</b></p>			
<p><b>Define and implement appropriate security controls for the relevant exchange of data. Where a system is used - system security management: Application of any requirements when setting up users.</b></p>			

Area of responsibility:	Joint Controller A:	Joint Controller B:	Joint Controller C:
<b>Encryption and pseudonymisation:</b> Determination of applicability as risk controls and implementation where possible.			
<b>Resilience and restoration:</b> Determination of applicability as risk controls and implementation where possible.			
<b>Security audits are undertaken:</b> Security controls as defined in the Data Protection Impact Assessment are audited to assure effectiveness.			
<b>Usage audits are undertaken.</b>			
<b>All access is by authorised users only:</b> Process to ensure all access is authorised.			
<b>Maintaining records of processing (ROPA):</b> Hold records of all data contributions and access controls.			
<b>Breach notification:</b> Notify any breaches to all affected partners and agree co-ordinated response.			

Area of responsibility:	Joint Controller A:	Joint Controller B:	Joint Controller C:
<b>Maintain any changes or additional processing.</b>			
<b>Audit risk control measures.</b>			
<b>Support data subject rights: Agree and maintain joint processes to support any requests related to shared data.</b>			



## 4 Processor(s)

Name of processor	Status		
	Controller(s) that Processor is processing data on behalf of.	Details of the data being processed or to be processed (what data, how is it being processed and why?).	Is an agreement (as per UK GDPR Article 28) in place between the Controller and Processor that covers the processing detailed above?
n/a			

## 5. Data shared between partners

---

- Adults have a general right to independence, choice and self-determination including control over information about themselves. In the context of preventing Crime and Disorder these rights can reasonably be overridden and personal, sensitive, non-sensitive and non-personal information shared without consent and without seeking consent in certain circumstances including:
  - other people are, or may be, at risk, including children
  - crime, disorder or ASB have been committed
  - sharing information could prevent crime, disorder or ASB
  - any party has, or may have, care and support needs and may be at risk of causing or being victim of crime, disorder or ASB.
  - a court order or other legal authority has requested the information.
  - emergency or life-threatening situations may warrant the sharing of relevant information with the relevant emergency services without consent.
- The law allows for sharing such information and agencies, their representatives and people working on their behalf are encouraged to do so in line with the principles within this document.
- Whilst information sharing is encouraged by this agreement, it is also important to apply a principle of only sharing the minimum amount of relevant information that is necessary to achieve the aim of preventing crime, disorder and ASB.
- This document represents an agreement/protocol between the Community Safety Partners in Bristol that sets out the processes and principles for sharing information between them and those working on their behalf.
- Due to the ability to share information members of the Community Safety Partnership and those working for them or on their behalf cannot give a personal assurance of confidentiality but can reassure individuals that information will only be the minimum amount of relevant information that is necessary to achieve the aim of preventing crime, disorder and ASB.
- Whilst it may be preferable to try gain the person's consent to share information, due to the often sensitive and risky nature of preventing crime, disorder and ASB it is recognized that this is often not practicable and therefore is not a barrier to information sharing.
- If it does not increase risk, practitioners should inform the person if they need to share their information without consent.

## Tier 2-Preventing Crime & Disorder Information and Data Sharing Agreement

- This agreement includes a clear escalation process to deal with any professional disagreements around sharing of information. It is important that the principles of this agreement are applied in settling any such disputes.
- All organisations will have a whistleblowing policy to allow for any abuse of this agreement to be highlighted.
- The management interests or political considerations of an organisation should not override the need to share information to prevent crime, disorder and ASB.
- All staff, in all partner agencies, should understand the importance of sharing information, take a proactive enabling approach to sharing and understand the potential risks of not sharing information.

## 6 Lawfulness – UK GDPR lawful basis and Article 9 conditions

---

a) UK GDPR

b) Data Protection Act 2018

c) Crime and Disorder Act 1998 UK Statutory Instrument 1831 The Crime and Disorder (Prescribed Information) Regulations 2007 Commissioners

Those who are commissioning services should consider whether contracts should place an obligation on service providers to share safeguarding information. Any specifications would need to be in line with policy, regulation, and the law. Individual agencies should have policies in place to deal with this.

Conditions for processing of personal data under UK GDPR

Compliance with the first principle 'Fair & Lawful Processing' ([UK GDPR Article 5\(a\)](#)) is achieved as follows:

- The processing satisfies the following **Processing Condition** within [UK GDPR Article 6\(1\)](#):

For Public Authorities

(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.

For Charities, Voluntary agencies and Private Businesses

(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.

Where **Special Category Data** is processed, in addition to a UK GDPR Article 6(1) Processing Condition being met, the following [UK GDPR Article 9\(2\)](#) **Special Processing Conditions** applies:

- (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;
- (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 referred to in paragraph 3

Where any of the following **Special Processing Conditions** (b), (h), (i) or (j) are chosen the following [DPA Schedule 1 Part 1](#) condition relating to employment, health & research etc applies:

- (2) Health or social care purposes

Where **Special Processing Condition** (g) is chosen the following [DPA Schedule 1 Part 2](#) substantial public interest condition applies:

- (6) Statutory etc and government purposes
- (10) Preventing or detecting unlawful acts
- (18) Safeguarding of children and of individuals at risk

Where a condition in DPA Schedule 1 Part 1 or 2 has been used an Appropriate Policy Document needs to be completed by each controller in accordance with DPA Schedule 1 Part 4

Where **Criminal Offence Data** is processed a compliance with [UK GDPR Article 10](#) an Appropriate Policy Document needs to be completed by each agency in accordance with DPA Schedule 1 Part 4, the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance.

## Sharing information on prisoners

The statutory guidance to the Care Act 2014 requires Local Authorities to share information about people with care and support needs in, or in transition from or to, prison or custodial settings. This includes *'the sharing of information about risk to the prisoner and others where this is relevant'*.

## Sharing information on those who may pose a risk to others.

The Police can keep records on any person known to be a target or perpetrator of abuse and share such information with safeguarding partners for the purposes of protection 'under Section 115 of the Crime and Disorder Act 1998, and the Data Protection Act 2018, provided that criteria outlined in the legislation are met'. All police forces now have ICT systems in place to help identify repeat and vulnerable victims of antisocial behaviour.

The statutory guidance to the Care Act 2014 states that Safeguarding Partnerships should:

*"have a framework and process for any organisation under the umbrella of the KBSP to respond to allegations and issues of concern that are raised about a person who may have harmed or who may pose a risk to adults"*.

Safeguarding Adult Lead Managers should 'ensure the control of information in respect of individual cases is in accordance with accepted Data Protection and Confidentiality requirements.

## Multi Agency Safeguarding Hubs

The KBSP are currently in the process of establishing an adult Multi Agency Safeguarding Hub (MASH) and will formalise arrangements for information sharing in the safeguarding context when this becomes operational. The purpose is to ensure that relevant information about potential safeguarding concerns in respect of adults (and children) is shared appropriately by the partner agencies where necessary. This enables the level of risk to be assessed appropriately and allows for suitable responses to be agreed.

As the MASH model is implemented more widely locally, separate information sharing agreements and protocols will need to be arranged to provide the basis for sharing information between the agencies engaged in the MASH in order to facilitate and govern the efficient, effective and secure sharing of timely and accurate information. It is acknowledged that the disclosure of any personal data must be bound to both common law and statute, for example defamation, the common law duty of confidence, the combined UK data protection laws (DPA 2018 & UK GDPR), and the Human Rights Act 1998.

## 6A Lawfulness - Data Protection Act 2018

### Complete the below if this activity includes processing for a law enforcement purpose

Law enforcement purposes are 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.

#### Avon & Somerset Constabulary

**Law Enforcement processing** as per DPA18, Section 30(1) is carried out by:

- **a competent authority (as per DPA18, Schedule 7), or**
- any other organisation with a statutory law enforcement function  
(*highlight which is appropriate*)

and

1. the data subject has given their consent for the processing, or
2. **the processing is necessary for a law enforcement purpose**  
(*highlight which is appropriate*)

**Law Enforcement processing of sensitive data** (processing of special category data under law enforcement processing) as per DPA18, Part 3, Section 35(2) can be carried out where:

1. the data subject has given their consent for the processing, or
2. **the processing is strictly necessary for a law enforcement purpose**
3. **and for both cases an appropriate policy document (APD) is in place**

if 2. strictly necessary for a law enforcement purpose

- The sensitive processing meets a legitimising condition in Schedule 8 of the DPA18 (*highlight from the below*)
  - **Statutory purpose**
  - Administration of justice
  - Vital interests
  - **Safeguarding children and adults at risk**
  - Data made public
  - Legal claims
  - Judicial acts
  - Preventing fraud
  - Archiving

**Probation, Prison Service, Local Authority:**

**Law Enforcement processing** as per DPA18, Section 30(1) is carried out by:

- a competent authority (as per DPA18, Schedule 7), or
- any other organisation with a statutory law enforcement function  
(*highlight which is appropriate*)

and

1. the data subject has given their consent for the processing, or
2. the processing is necessary for a law enforcement purpose(*highlight which is appropriate*)  
(*highlight which is appropriate*)

**Law Enforcement processing of sensitive data** (processing of special category data under law enforcement processing) as per DPA18, Part 3, Section 35(2) can be carried out where:

1. the data subject has given their consent for the processing, or



2. the processing is strictly necessary for a law enforcement purpose
3. and for both cases an appropriate policy document (APD) is in place

if 2. strictly necessary for a law enforcement purpose

- The sensitive processing meets a legitimising condition in Schedule 8 of the DPA18 (*highlight from the below*)
  - Statutory purpose
  - Administration of justice
  - Vital interests
  - Safeguarding children and adults at risk
  - Data made public.
  - Legal claims
  - Judicial acts
  - Preventing fraud
  - Archiving

## 6B Lawfulness – legal powers and gateways

Data protection law requires data sharing to be lawful. An organisation needs to have a power to share data which may lie either in statute or in common law. The functions of a public sector organisation are set out in legislation, often referred to as 'legal powers and gateways'. Effective performance of those functions often requires the sharing of relevant personal and special category data. For some organisations the power to share data lies solely in common law although this is unlikely for public sector organisations. Knowing the legislation and common law duty or power that links to the relevant functions of safeguarding will provide a framework to enable the sharing of data to safeguard and protect children.

The detail of the relevant legislative powers may affect how we meet a data subject's rights. For example, where there is a duty to perform a function and that can't be performed without relevant personal data, a data subject objecting to the processing may be told there are compelling legitimate reasons why their objection cannot be upheld. For example, if a data subject requested that notes are not taken and shared of a case conference meeting.

Below is a list of legislation relevant for the processing/sharing of information between local authorities and their partners. This is not a full list of all relevant legislation but the most commonly used ones for sharing scenarios involving local authorities. It is important that the correct legal gateway is identified to establish grounds for processing/data sharing depending on the particular circumstances.

Relevant Act	Relevant Section	Content	Partners the Legislation is relevant for
Care Act 2014	Section 1	Duty on Local Authorities to promote an individual's well-being including: (a) personal dignity (including treatment of the individual with respect); (b) physical and mental health and emotional well-being; (c) protection from abuse and neglect; (d) control by the individual over day-to-day life (including over care and support, or support, provided to the individual and the way in which it is provided);	Local Authority

		<p>(e)participation in work, education, training or recreation;                  (f)social and economic well-being;                  (g)domestic, family and personal relationships;                  (h)suitability of living accommodation;                  (i)the individual’s contribution to society.</p> <p>with regard to a number of matters including                  (d)the need to ensure that decisions about the individual are made having regard to all the individual’s circumstances (and are not based only on the individual’s age or appearance or any condition of the individual’s or aspect of the individual’s behaviour which might lead others to make unjustified assumptions about the individual’s well-being);</p>	
Care Act 2014	Section 2	The Local Authority must prevent needs for care and support by arranging for the provision of services, facilities or resources, or take other steps.	Local Authority
Childcare Act 2006	Section 1	<p>General duties of local authority in relation to well-being of young children including the improvement of well-being of young children in the local authority area, and reduce inequalities between young children in their area in relation to the matters as follows:</p> <p>(a)physical and mental health and emotional well-being;                  (b)protection from harm and neglect;                  (c)education, training and recreation;                  (d)the contribution made by them to society;                  (e)social and economic well-being.</p>	Local Authority
Crime and Disorder Act 1998	Section 115	<p>Disclosure of information.                  (1)Any person (educational settings) who, apart from this subsection (e.g. LA &amp; Police), 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</p>	Educational Setting

		any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.	
Crime and Disorder Act 1998	Section 17	Duty on authorities to consider crime and disorder implications by doing what it reasonably can to prevent: (a)crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment); and (b)the misuse of drugs, alcohol and other substances in its area; and (c)re-offending in its area]	Police, Local Authority
Crime and Disorder Act 1998	Section 37	37Aim of the youth justice system. (1)It shall be the principal aim of the youth justice system to prevent offending by children and young persons. (2)In addition to any other duty to which they are subject, it shall be the duty of all persons and bodies carrying out functions in relation to the youth justice system to have regard to that aim.	Police, Local Authority
Criminal Justice Act 2003	Section 325	The responsible authority for each area must establish arrangements for the purpose of assessing and managing the risks posed in that area by— (a)relevant sexual and violent offenders, and (b)other persons who, by reason of offences committed by them (wherever committed), are considered by the responsible authority to be persons who may cause serious harm to the public. (3)In establishing those arrangements, the responsible authority must act in co-operation with the persons specified in subsection (6); and it is the duty of those persons to co-operate in the establishment by the responsible authority of those arrangements, to the extent that such co-operation is compatible with the exercise by those persons of their relevant functions. (4)Co-operation under subsection (3) may include the exchange of information.	Police, Local Authority
Education Act 2002	Section 175	Duties in relation to welfare of children (1)A [F2local authority] shall make arrangements for ensuring that [F3their education functions] are exercised with a view to safeguarding and promoting the	Educational Settings, Local Authorities

		<p>welfare of children.</p> <p>(2)The governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.</p> <p>(3)The governing body of an institution within the further education sector shall make arrangements for ensuring that their functions relating to the conduct of the institution are exercised with a view to safeguarding and promoting the welfare of children receiving education or training at the institution.</p> <p>The safeguarding duties” are—</p> <p>(a)a duty to make arrangements to ensure that the proprietor's functions relating to the conduct of the institution are exercised with a view to safeguarding and promoting the welfare of children receiving education or training at the institution.</p>	
Education Act 2002	Section 157	<p>Independent schools only, including academies and CTCs)</p> <p>(1)For the purposes of this Chapter, regulations shall prescribe standards about the following matters—</p> <p>(a)the quality of education provided at independent schools;</p> <p>(b)the spiritual, moral, social and cultural development of pupils at independent schools;</p> <p>(c)the welfare, health and safety of pupils at independent schools;</p> <p>(d)the suitability of proprietors of and staff at independent schools;</p> <p>(e)the premises of and accommodation at independent schools;</p> <p>(f)the provision of information by independent schools;</p> <p>(g)the manner in which independent schools handle complaints.</p>	Educational Settings
The Education (Independent Schools Standards)	Schedule 'The Independent Schools	<p>Independent schools only, including academies and CTCs)</p> <p>Welfare, health and safety of pupils</p> <p>3.—(1) The welfare, health and safety of pupils at the school meets the standard if</p>	Educational Settings, Local Authorities through DfES (guidance only)

<p>(England) Regulations 2003</p>	<p>Standards, Section 3</p>	<p>the requirements in sub-paragraphs (2) to (9) are met.</p> <p>(2) The school shall draw up and implement effectively a written policy to—</p> <p>(b)safeguard and promote the welfare of children who are pupils at the school, which complies with DfES Circular 10/95 “Protecting Children from Abuse: the Role of the Education Service”;</p> <p>(c)safeguard and promote the health and safety of pupils on activities outside the school, which has regard to DfES Guidance “Health and Safety of Pupils on Educational Visits(8)”;</p>	
<p>The Children Act 2004</p>	<p>Section 10</p>	<p>Each local authority must make arrangements to promote co-operation between partners (including the CCG, Police, Schools and other) to improve the well-being of children including:</p> <p>(a)physical and mental health and emotional well-being;</p> <p>(b)protection from harm and neglect;</p> <p>(c)education, training and recreation;</p> <p>(d)the contribution made by them to society;</p> <p>(e)social and economic well-being.</p>	<p>Local Authority</p>
<p>The Children Act 2004</p>	<p>Section 11</p>	<p>Arrangements to safeguard and promote welfare (this section applies to partners including the CCG, Police and Schools).</p>	<p>Local Authority, Police, Probation, Youth Offending Team</p>
<p>Welfare Reform Act 2012</p>	<p>Section 131</p>	<p>Information -sharing in relation to welfare services (including the Local Authority and Schools) and for prescribed purposes relating to welfare services.</p> <p>Section 131 restores and widens powers for the DWP to share information with local authorities in relation to welfare services and section 134 allows for longer term data sharing powers between DWP, their service providers and local authorities in particular to those working with troubled families and their in work and out of work benefits.</p>	<p>Local Authority, Educational Setting</p>

Education and Skills Act 2008	Section 68	Provision of support services by local authorities to support for participation in education or training, young adult with learning difficulties and young people in England.	Local Authority, Educational Setting
Domestic Abuse Statutory Guidance July 2022	Section 248	Police notify schools about all domestic abuse incidents before the start of the next school day.	Police, Local Authority, Educational Settings
Domestic Abuse Statutory Guidance July 2022	Section 439	Everyone who works with children has a responsibility for keeping them safe and that multi-agency working, and information sharing is essential to ensure that children and families receive the right help at the right time.	Police, Local Authority, Educational Settings
Domestic Abuse Statutory Guidance July 2022	Section 443	For multi-agency working to be effective, all agencies must work with a clear and common focus. For this to be achieved partnerships should: ... Share information in a way that is timely, proportionate, legal, and safe.	Police, Local Authority, Educational Settings
Domestic Abuse Statutory Guidance July 2022	Section 445	Effective and meaningful multi-agency work relies heavily on timely and appropriate, while lawful, information sharing, ensuring all agencies have the necessary information to participate materially in meetings and make informed decisions.	Police, Local Authority, Educational Settings
Childcare Act 2006	Section 3	Describes specific duties of local authority in relation to early childhood services. The authority must make arrangements to secure that early childhood services in their area are provided in an integrated manner which is calculated to- (a) Facilitate access to those services, and (b) maximise the benefit of those services to parents, prospective parents and young children.	Police, Local Authority
Children (Leaving Care) Act 2000		The main purpose of the Children (Leaving Care) Act is to improve the life prospects of young people who are looked after by Health and Social Care Trusts as they make the transition to independent living.	Local Authority
The Children Act 1989	Part 3	Each local authority has a duty to "safeguard and promote the welfare" of children who are assessed as being in need. A child is deemed as "in need" if they are disabled or unlikely to achieve a reasonable standard of health or development	Local Authority

		<p>unless services are provided.</p> <p>s17 (General duty of local authority to safeguard and promote welfare of children in their area who are in need)</p> <p>s27 (local authority ability to request help and assistance in complying with the s17 duty from other authorities and corresponding duty to comply with such a request)</p> <p>s47 (Local authority duty to investigate where there is reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm)</p> <p>s1(1) of Schedule 2 (Duty of local authority to take reasonable steps to identify the extent to which there are children in need within their area)</p>	
Localism Act 2011		<p>The Localism Act includes a ‘general power of competence’. It gives local authorities the legal capacity to do anything that an individual can do that is not specifically prohibited. The new, general power gives councils more freedom to work together with others in new ways to drive down costs. It gives them increased confidence to do creative, innovative things to meet local people’s needs. Councils have asked for this power because it will help them get on with the job. The general power of competence does not remove any duties from local authorities - just like individuals they will continue to need to comply with duties placed on them.</p>	Local Authority
Local Government Act 2000	Section 2	<p>This gives local authorities ‘a power to do anything which they consider is likely to achieve any one or more of the following objectives’:</p> <p>(a) The promotion or improvement of the economic well-being of their area</p> <p>(b) The promotion or improvement of the social well-being of their area</p> <p>(c) The promotion or improvement of the environmental well-being of their area</p> <p>Section 3 is clear that local authorities are unable to do anything (including sharing</p>	Local Authority



		data) for the purposes of the well-being of people – including children and young people – where they are restricted or prevented from doing so on the face of any relevant legislation, for example, the Human Rights Act, the Data Protection Act or by the common law duty of confidentiality.	
Children and Family Act 2014	Section 23 & 25	<p>The Children and Families Act 2014 makes provision to reform the law relating to care and support for children with special educational needs or a disability.</p> <p>Section 23 places a duty on health bodies 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. 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 provision and social care provision where it thinks that this would –</p> <p>promote the well-being of children or young people in its area who have special education needs or a disability, or</p> <p>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.</p>	Health bodies and local authorities
Health and Social Care (Quality & Safety) Act 2015	Section 3	<p>Section 3 (1),(2)(a)(b):</p> <p>(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”).</p> <p>(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.</p>	All commissioners and providers of health and care services to adults.
Health & Social Care Act 2012	Section 195	<p>Section 195:</p> <p>(contains guidance about) specific duties of co-operation, including creating a Health and Wellbeing Board, which must, for the purpose of advancing the health</p>	All commissioners and providers of

		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.	health and care services.
National Health Service Act 1977	Section 22	Co-operation between health authorities and local authorities. (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 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
Management of Police Information (MoPI) statutory Code of Practice		The Management of Police Information (MoPI) statutory Code of Practice provides a framework for the processing of police information (including intelligence and personal data obtained and recorded for police purposes). Policing purposes are: a) protecting life and property, b) preserving order, c) preventing the commission of offences, d) bringing offenders to justice, and e) any duty or responsibility of the police arising from common or statute law.	Police

<p>Children and Social Care Work Act 2017</p>	<p>Part 1, Chapter 2, 19</p>	<p>Information                      (1)Any of the safeguarding partners for a local authority area in England may, for the purpose of enabling or assisting the performance of functions conferred by section 16E or 16F, request a person or body to provide information specified in the request to—                      (a)the safeguarding partner or any other safeguarding partner for the area,                      (b)any of the relevant agencies for the area,                      (c)a reviewer, or                      (d)another person or body specified in the request.                      (2)The person or body to whom a request under this section is made must comply with the request.                      (3)The safeguarding partner that made the request may enforce the duty under subsection (2) against the person or body by making an application to the High Court or the county court for an injunction.                      (4)The information may be used by the person or body to whom it is provided only for the purpose mentioned in subsection (1).”</p>	<p>Local Authority and Safeguarding Partners</p>
---	------------------------------	--	--

## 7 Non-Interference – Common law duty of confidentiality

Non-interference with the common law duty of confidentiality describes the duty we have, to keep personal information confidential under case law (not written out in a document (e.g., an Act) but based on previous court cases decided by judges). The law is applied by reference to those previous cases, so common law is also said to be based on precedent. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed unless it is lawful because 1) the individual has given consent, 2) where it is necessary to safeguard the individual, or others, or it is in the wider public interest, 3) where there is a legal duty to do so.

Please state here and explain how you will be satisfying Confidentiality:

**1) Consent\*:** N/A

**2) Substantial Public Interest:** Sharing initiative is based on the public interest to Safeguard children and individuals at risk, to prevent crime and disorder and improve community safety.

**3) Legal duty:** N/A

\* Please note that consent under the common law is not the same as consent under data protection law. Consent under data protection law must be freely given, specific, and involve an affirmative action (UK GDPR Article 7 compliance). Consent under common law is satisfied if the individual(s) are aware and not objecting. This is 'implied' consent. Data Protection legislation requires individuals to be informed (see section 8) and allows them the opportunity to object (see section 9).

## 7A Non-Interference – Human Rights Act 1998, Article 8

Non-interference with Article 8 of the Human Rights Act 1998 guarantees the protection of individuals right to respect for private and family life, home and correspondence.

### Please state here if there is any interference with the Human Rights Act 1998, Article 8

**Yes:**

Local Authorities might be able to interfere with the right if the action is lawful, necessary and proportionate in order to:

- protect public safety
- protect health or morals
- prevent disorder or crime, or

*(if yes, why is it necessary and proportionate to share/process data)*

*To enable partner agencies to make informed decisions on where to prioritise resources to help tackle crime and disorder. This could be through identification of particular problem areas or through direct work with individuals. Without sharing agencies will not have access to the full details and could miss opportunities to tackle criminality and this could impact on the wider community as well as placing vulnerable people at greater risk of harm.*

*The Crime and Disorder Act places a statutory duty on relevant authorities to address these concerns and this overrides Article 8 – Right to Private and Family Life – where appropriate.*

**No:**

## 8 Transparency

Being open and honest with individuals whose data is shared/processed is a key requirement under current UK data protection legislation and one of the rights an individual is entitled to under the UK GDPR. Transparency gives individuals greater control of the data organisations hold on them and it is an essential exercise sharing partners must consider and comply with.

**Have Privacy Notices been updated to reflect the details around the sharing initiative (add more organisations as/if required)?**

**Avon & Somerset Constabulary's Privacy Notice already covers this level of Information Sharing. [Privacy Notice](#)**

Bristol City Council has a Privacy Notice under the Keeping Bristol Safe Partnership covering this level of Information Sharing. [Privacy Notice Article 4](#)

Bristol, North Somerset and South Gloucestershire Integrated Care Board (BNSSG ICB). [How we use your information - NHS BNSSG ICB](#) [Our uses of information - NHS BNSSG ICB](#)

Avon Fire & Rescue Service (AF&RS) there are also separate drop downs for specific areas and one of these covers Safeguarding and types of external organisations we may share data with <https://www.avonfire.gov.uk/privacy/>



Probation Service  
Privacy Notice.pdf

**Is privacy information shared in a timely manner?**

**Include when data is collected directly from the individual & if contained from source other than individual.**

Avon & Somerset Constabulary– Details recorded on Privacy Notice.

Bristol City Council – Details recorded on Privacy Notice.

BNSSG ICB – Details recorded on Privacy Notice

Avon Fire & Rescue Service (AF&RS) - details recorded on Privacy Notice on website. For information obtained via a Home Fire Safety Visit (HFSV) process, there is a privacy statement in the HFSV booklet provided to the individual.

Probation Service – details recorded on Privacy Notice.

**What other tools are in place to comply with transparency?**

Avon & Somerset Constabulary– Details recorded on Privacy Notice.

Bristol City Council – Details recorded on Privacy Notice.

BNSSG ICB – Details recorded on Privacy Notice.

Avon Fire & Rescue – details recorded on Privacy Notice.

Probation Service – details recorded on Privacy Notice

## 9 Individuals' rights

The UK data protection legislation provides a number of rights to individuals whose data is being processed/shared. Organisations are legally obliged to assure those rights are supported.

**Each organisation is to have their own processes in place to enable data subjects to exercise their information rights:**

**The right of access**

**The right of rectification**

**The right to restrict processing**

**The right to object**

**Rights in relation to automated decision making and profiling**

The right to be informed is covered under '8 Transparency' of this document.

Some rights may not apply depending on the lawful basis information/data is processed under. When processing/sharing information for reasons of safeguarding, it is likely that organisations will do so under the 'legal obligation' or 'public task' basis. The following rights will therefore not apply: right to erasure, right to portability, right to object (applies for public task but not for legal obligation).

Some of the rights may not be applicable where data is processed for a law enforcement purpose.

Please note and consider that private or third sector organisations (e.g., charities) are likely to use the 'legitimate interest' basis where the relevance of individual rights will differ).



## 10 How data sharing will be carried out

---

This section should detail the approaches used to share data, which may be manual/procedural, potentially supported by technical solutions e.g., data will be shared 'face to face' at a multi-disciplinary meeting, where each partner brings their relevant records, such meetings may also be supported by technical solutions (e.g. manual upload of documents to shared space (cloud-based fileserver/MS Teams etc.), by automated data transfer from system to system, via email or other).

It should also be documented:

- How data is protected during transit e.g., SFTP (Secure File Transfer Protocol), upload/download to/from https or network accessed through VPN, encrypted email, etc. For the DSA this may be a brief overview, with detail in the Data Protection Impact Assessment (DPIA).
- The organisation(s) responsible for ensuring security i.e., one organisation may have developed/implemented a web application, a cloud-based fileserver, etc, for multiple organisations to use to share data.
- The frequency of sharing i.e., daily, once a week, once a month, etc, and extent of data shared each time i.e., new data, updates/changes since last data share.

**The approach or mechanism/method by which data will be shared:**

**Avon & Somerset Constabulary Dataset:** Automated data transfer of an agreed dataset to a Secure File Transfer Location. (Technical detail is assessed in the Data Protection Impact Assessment)

**Regular 'case-by-case' information sharing:** This includes numerous information sharing mechanisms including, but not limited to: written communications (emails, online messaging platforms (e.g. Teams)) and verbal communication (face-to-face, telephone, video calls).

**Information sharing in multi-agency meeting settings:** Information is shared verbally during such meetings and in written format in the agenda/minutes/any other supporting documentation.

**Protection of data in transit:**

**Avon & Somerset Constabulary Dataset:** Encrypted data transfer (detail in the DPIA)

**Regular 'case-by-case' information sharing:** Where verbal communications are being utilised, it is the responsibility of all parties to ensure the information being shared cannot be overheard by third parties. Where written communication is being utilised, it is the responsibility of the sender to use secure methods and/or pseudonymise those communications in so far as is reasonably practicable.

**Information sharing in multi-agency meeting settings:** It is the responsibility of the attendees at such meetings to ensure that verbal communications cannot be overheard by third parties. It is the responsibility of the person sharing any written material to use secure methods and/or pseudonymised that material in so far as is reasonably practicable.

**Organisation(s) responsible for the security of data:**

**Avon & Somerset Constabulary Dataset:** All data will be securely held within BCCs Azure cloud tenant where possible.

**Regular 'case-by-case' information sharing:** It will be the responsibility of the agency who is transmitting the information to ensure that they are transmitting it to an organisation covered by this document. It will be the responsibility of the receiving organisation to ensure data is stored securely.

**Information sharing in multi-agency meeting settings:** It will be the responsibility of the agency who is transmitting the information to ensure that they are transmitting it to an organisation covered by this document. It will be the responsibility of the receiving organisation to ensure data is stored securely. All attendees at such meetings should be invited to agree to an information sharing statement that sets out the basis for sharing the information (e.g. preventing crime and disorder, managing risk to public) but that information will not be shared onwards without the consent of the organisation bringing the information.

#### Frequency and extent of sharing:

**Avon & Somerset Constabulary Dataset:** Updates/changes to the data on a weekly basis

**Regular 'case-by-case' information sharing:** Information will be shared as and when necessary for the purposes of preventing crime and disorder.

**Information sharing in multi-agency meeting settings:** Information sharing will occur in line with frequency of such settings.

#### If data is being transferred outside the UK:

*See 11*

# 11 Processing outside of the UK (Compliance with Article 45 of the UK GDPR)

---

Transferring personal data outside the UK comes with the responsibility of following the relevant rules and safeguards to facilitate such transfers. Please refer to the available ICO guidance and checklist [here](#). Please state below if any personal data will be transferred outside the UK. Advice from the DPO will be required for any potential transfers.

**1. Will any of the personal data be transferred outside of the UK?**

No

**2. If yes, please state where the data will be transferred to:**

If outside the European Economic Area (EEA) please complete section 3 below.

**3. If yes, please give details and explain how it is ensured that appropriate safeguards are in place:**

## 12 Accuracy of data before sharing

Each sharing partner is responsible for ensuring the accuracy of the personal data that it shares and must have robust processes in place for managing data quality. Describe the processes for ensuring that information/data held and shared is accurate and relevant (e.g., testing, quality checks, removal of duplicates, review and testing of algorithms, data validation in data fields and exchanges etc.). This document should give an overview of this element, detail as required can be included in any related Data Protection Impact Assessment (DPIA).

This is key for any sharing that is facilitated by a data system/application, but also important for data sharing that is manual/procedural (such as via a multidisciplinary team (MDT)), although in such cases often reliant on organisational operational processes for the accurate recording of data.

### **Avon & Somerset Constabulary Dataset:**

- Data quality checks are carried out upon refreshing the data on a weekly basis.
- When end users identify instances of inaccuracy in the data, this is reported to the Insight team. The Insight team can then go to the data source controller and make them aware of the inaccuracy.
- When developing new reports these are tested first in a TEST environment to ensure the data is reflective of what it is expected. Once a report is doing as intended it will be published to LIVE and subject to further testing
- Any significant increase/decrease in trends is checked with Avon & Somerset Constabulary Data and Insight Team, to understand whether these are genuine changes or due to changes in reporting practices

### **General, case-by-case or multi-agency setting sharing:**

Each agency will be responsible for checking that the information they are sharing is accurate and, if it becomes apparent that it is not then they will be responsible for informing relevant partners as soon as is reasonably practicable. Each agency will utilise its own organisational processes that relate to accurate data recording. Each agency will consider providing further detail in any related DPIA.

## 13 Rectification of data that has been shared

---

Specify here any procedures in place, or to be put in place, for rectifying the sharing of inaccurate data. Explain how any updates will be shared with all recipients of the data.

### Explain how any updates will be shared with all recipients of the data:

Each organisation is responsible for ensuring that the information provided is accurate; and any inaccurate data identified is notified to the other organisations as soon as it is discovered to be inaccurate.

#### **Avon and Somerset Constabulary regular data sharing:**

- When end users identify instances of inaccuracy in the data, this is reported to the Insight team. The Insight team can then go to the data source controller and make them aware of the inaccuracy.
- Weekly Snapshots are sent to all recipients of the data- this can be amended to notify recipients of any updates with regards to the rectification of inaccurate data

*Note:* Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared. If a rectification request comes directly from a data subject, please refer to section 9 Individuals' Rights..

## 14 Retention and disposal

---

Organisations are required by law to not retain information/data for longer than necessary for the purpose(s) for which it was collected. Partners must follow their organisational policies and procedures whilst adhering to statutory requirements. The deletion and disposal of information/data must be done securely with the appropriate safeguards in place. Consultation with Records Management or the Information Governance Team is advised.

Where organisations are sharing data into a shared repository then they will likely need to consider if there is any difference in retention periods and decide which will apply. Where data is exchanged, i.e., copies of data passed between organisations, then the recipient of the copy is responsible for managing their retention of it (as agreed between the relevant parties).

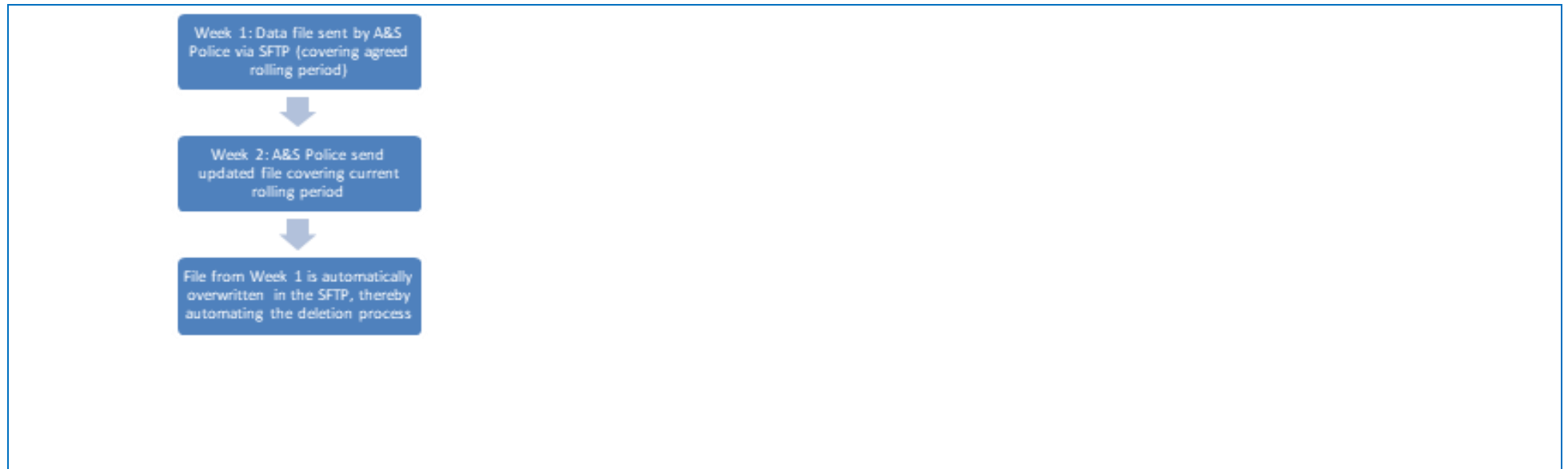
### State each relevant organisation's retention periods relating to the data processed/shared under this DSA:

All organisations will follow their own data retention periods.

### State how each organisation complies with the required safeguards when deleting/disposing of the data processed/shared under this DSA:

All organisations will follow their own policies and processes when deleting/disposing of data.

### Avon & Somerset Constabulary regular data sharing:





## 15 Breach management

---

All relevant parties must have clear policies, procedures, and processes in place to manage Data Protection Incidents and Breaches in compliance with the current UK data protection legislation. If any incidents occur, then they will initially be managed by the incident management policy of the party identifying the breach. If they are joint controllers these procedures must be set out in the joint controller responsibility section of this template as per Article 26 of the UK GDPR (see under 3). If there is a controller-processor relationship this must be set out in the contract as per Article 28 of the UK GDPR (see under 4).

The first stage of investigation is to identify which organisation appears to be responsible for the circumstances leading to the breach. In many cases this can be established quickly and where this is not the organisation that has identified the breach, then the organisation(s) that appears responsible will take over the investigation.

Where the responsible organisation is not the original controller of the data that has been breached, then the responsible organisation will contact each and every controller whose data appears to be part of the breach to keep them informed of the investigation and all parties will collaborate as needed to support the investigation and any required remedial and safeguarding actions.

This includes assessing the need to report, where required, to the supervisory authority (ICO notification must be done within 72 hours of becoming aware of the breach, where feasible) and, where required, the affected data subjects.

### Document any specific arrangements here (if applicable):

**Avon & Somerset Constabulary:** Ensure only staff and partners familiar with appropriate data sharing principles are granted access. Use Row-Level Security to ensure only appropriate persons have access to Power BI dashboards. Minimise person-level sharing through other formats- through ensuring that snapshots or extracts of dashboards contain anonymized data only.

All breaches to be reported to [DPABreaches@avonandsomerset.police.uk](mailto:DPABreaches@avonandsomerset.police.uk)

All breaches involving Bristol City Council service user data should immediately be reported to [data.breach@bristol.gov.uk](mailto:data.breach@bristol.gov.uk)

All breaches to be reported to [bnssg.data.protection@nhs.net](mailto:bnssg.data.protection@nhs.net)

All breaches involving Avon Fire & Rescue Service user data to be reported to our Service Control on 0117 9262061 ext. 311/312. Service Control will then log as an incident and contact the Duty Group Manager. Please also email [DPO@avonfire.gov.uk](mailto:DPO@avonfire.gov.uk) and AF&RS Lead Officer to this Agreement

All breaches of Probation data should be reported to [DPO@justice.gov.uk](mailto:DPO@justice.gov.uk)

## 16 IG Contacts

List the relevant Information Governance Contacts here including the Caldicott Guardian, Data Protection Officer and Senior Information Risk Owner (SIRO) as appropriate.

Organisation	Name	Role	Contact details
Avon & Somerset Constabulary	Kevin Coe	Information Governance Manager	<a href="mailto:DPO@avonandsomerset.police.uk">DPO@avonandsomerset.police.uk</a>
Bristol City Council	Ben Hewkin	Head of Information Assurance	<a href="mailto:Data.protection@bristol.gov.uk">Data.protection@bristol.gov.uk</a>
BNSSG ICB	Dr Joanne Medhurst	Caldicott Guardian	<a href="mailto:BNSSG.foi@nhs.net">BNSSG.foi@nhs.net</a>
Avon Fire and Rescue Service	Lucy Jefferies	Information Governance Manager	<a href="mailto:FOI-DP@avonfire.gov.uk">FOI-DP@avonfire.gov.uk</a>
Probation Service	Claire Summers	Information Asset Custodian	<a href="mailto:claire.summers@justice.gov.uk">claire.summers@justice.gov.uk</a>

## 17 Review

---

It is important to build in regular reviews at appropriate intervals to assure any relevant changes have been considered within the document.

**State when the agreement will be reviewed, the role of the person who will conduct the review and how it is planned to be undertaken, noting any consultation requirements such as with stakeholders, data subjects and the wider public.**

This agreement will be reviewed annually unless a significant event (e.g. legislative changes) requires a more urgent review. All reviews will be co-ordinated by the Keeping Bristol Safe Partnership.

## 18 Variation

---

**State here if the any party can vary the terms of this agreement. Describe how this will be done and how agreement on variation will be reached. If not required this section does not need to be included:**

Any party can request variation of the terms of this agreement by contacting [KBSP@bristol.gov.uk](mailto:KBSP@bristol.gov.uk)

## 19 Ending the agreement.

---

State how a party can end their participation in the agreement, and how data shared by the exiting party will be managed. Where data is shared into a system/application, the data feed will likely be turned off and a decision on previously shared data needs to be made, both from a legal perspective but also a risk/safety perspective. If data has been shared between parties as an exchange, then it needs to be agreed what will happen.

**State how a party can end their participation in the agreement, and how data shared by the exiting party will be managed:**

Any party can end their participation in the agreement at any point by contacting [KBSP@bristol.gov.uk](mailto:KBSP@bristol.gov.uk).

## 20 End date

---

You may have a planned date to stop sharing, especially if there is a finite project. If the sharing is expected to be ongoing, you can state this.

**State the date the agreement ends and how data will be managed:**

This agreement has no end date but can be reviewed or withdrawn from as per sections 19 and 20 above.

## 21 Signatories

---

Each organisation must sign here. Give the name and position of the signatory based on the sharing required. For example: DPO, SIRO, CG, CEO, Head of Service.

By signing this DSA, all signatories acknowledge and accept the requirements placed upon them and others within their organisations by the DSA and their responsibilities under data protection legislation.

### 1. Signed on behalf of: Bristol City Council

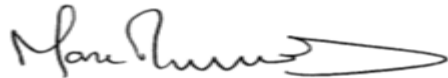
**By:** Christina Gray, Director of Communities and Public Health



**Date signed:** 26/11/2024

### 2. Signed on behalf of: Avon and Somerset Constabulary

**By:** Mark Runacres, Superintendent, Bristol Police Commander



**Date signed:** 19/12/2024

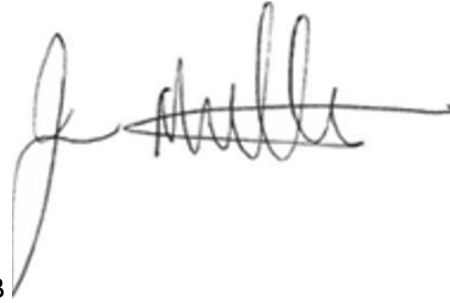
### 3. Signed on behalf of: Avon Fire & Rescue

**By:** Nikki Rice, Vulnerable Adults Manager & Joint Safeguarding Lead



**Date signed:** 10/12/2024

4. Signed on behalf of: Bristol North & South Gloucestershire Integrated Care Board (BNSSG ICB)


A handwritten signature in black ink, appearing to read 'J Medhurst', written over a horizontal line.

**By:** Dr Joanne Medhurst – Caldicott Guardian BNSSG ICB

**Date signed:** 21/11/2024

5. Signed on behalf of: Ministry of Justice (incs: HM Prison & Probation Service, Courts and Tribunal Judiciary)

**By:** Claire Summers, Head of Bristol & South Gloucestershire PDU

A handwritten signature in black ink, appearing to read 'C Summers', written over a horizontal line.

**Date signed:** 18/12/2024

The Keeping Bristol Safe Partnership Business Unit manages the full list of signatories to this agreement.

## 22 Abbreviations and glossary

Term	Definition
Ad-hoc data sharing	Information sharing outside a formal meeting or system, often on a one-off basis.
Appropriate Policy Document (APD)	An appropriate policy document is a short document outlining your compliance measures and retention policies. It is required under the Data Protection Act 2018 for some of the conditions documented in Schedule 1 (Part 1, 2 and 3).
Caldicott Guardian	A senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian. Further, guidance has been issued under the Health and Social Care (National Data Guardian) Act 2018 that recommends "other organisations providing services as part of the publicly funded health service, adult social care, or adult carer support" should have a Caldicott Guardian by 30/06/2023: <a href="https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf">https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf</a>
Commissioning Support Unit (CSU)	CSUs are organisations whose primary purpose is to provide Integrated Care Boards with external support, specialist skills and knowledge to support them in their role as commissioners. They were established following the changes brought about by the Health and Social Care Act 2012, to support Clinical Commissioning Groups (now ICBs) after Primary Care Trusts were retired. However, CSUs have evolved to provide a much wider array of services, with a broad portfolio, such as supporting national programmes and providers of all types.



Term	Definition
Common law duty of confidentiality	The common law duty of confidentiality is not codified; it is based on previous judgements in court. Whilst various interpretations of the common law may be possible it is widely accepted that, where information which identifies individual service users is provided and held in confidence, disclosure may only be justified in <u>one</u> of three ways: <ol style="list-style-type: none"> <li>1. the service user has given consent for their information to be used;</li> <li>2. the balance of public and private interest favours public interest disclosure; or</li> <li>3. a statutory basis exists which permits or requires disclosure.</li> </ol> (source: Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016, Explanatory Note, Common Law Duty of Confidentiality)
Criminal Offence Data	Includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.
Data	The use of data in this document must be understood as information which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Data Controller / Joint Controller	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.
Data Protection Act (DPA) 2018	The DPA 2018 sits alongside and supplements the UK GDPR.
Data Protection Impact Assessment (DPIA)	A process to help you identify and minimise the data protection risks related to processing of personal data. A DPIA is legally required in some circumstances.
Data Protection Officer (DPO)	The primary role of the data protection officer (DPO) is to ensure that their organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
Data Subject	The individual to whom the data being processed relates and is identified/identifiable by that data.
Data Sharing	Data sharing as used within this document can be understood as sharing of personal data.

Term	Definition
Data Sharing Agreement (DSA)	Terminology can vary (Data Sharing Protocol, Data Sharing Contract, Personal Data Sharing Agreement) but can be used interchangeably in the guidance. A DSA can be used between sharing partners (Controllers) to help demonstrate compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality and other relevant laws. It should help you justify your data sharing, clarify responsibilities of the sharing partners and set agreed parameters for the use of data.
Department for Work and Pensions (DWP)	The DWP is responsible for welfare, pensions and child maintenance policy.
Department of Education (DoE)	The Department for Education is responsible for children’s services and education, including early years, schools, higher and further education policy, apprenticeships, and wider skills in England.
European Economic Area (EEA)	The EEA includes EU countries and Iceland, Liechtenstein, and Norway. The UK has adequacy regulations in place about these countries (expected to last until 27 June 2025).
ICO Registration Number	Number attributed to an organisation that meets the legal requirement to register with the ICO.
Information	The use of information in this document must be understood as organised data providing context which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Information Commissioner’s Office (ICO)	The UK’s independent body set up to uphold information rights.
Law Enforcement Processing	Processing (including sharing) of personal data by competent authorities (for definition click <a href="#">here</a> ) for a Law Enforcement Purpose.
Law Enforcement Purposes	As defined by Section 31 Data Protection Act 2018 - 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 (for details click <a href="#">here</a> ).
Legal gateway	Legislation and common law that establishes justifiable grounds for the processing of personal data.

Term	Definition
Local Authority (LA)	An LA is a local government organisation responsible for the administration of government policy at a local level.
Means [of processing]	Actions taken in the processing of data to achieve the purpose(s) for its processing i.e. how the data is processed but can also be considered to extend to what data is used to achieve the purpose(s).
Modelling	The application of structured analysis, or use, of data.
Multi-Agency Safeguarding Hub (MASH)	The Multi-Agency Safeguarding Hub (MASH) brings key professionals together to facilitate early, better quality information sharing, analysis, and decision-making, to safeguard vulnerable children and young people more effectively.
Personal data	Data that relates to a living identified or identifiable individual.
Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Purpose(s) [of processing]	Reasons to process personal data.
Risk Scoring	The application of a value/score based on a set of relevant risk factors and calculations/algorithms
Role-based access control (RBAC)	A model for controlling access to resources (i.e., data) where permitted actions on resources are identified with roles. (e.g., an employee with a health/care professional role may access full service user health/care records, whilst a health/care service administrator may only access limited details from service user health/care records).
Secure File Transfer Protocol (SFTP)	A protocol for securely accessing and transferring large files across the web.
Senior Information Risk Owner (SIRO)	The SIRO is responsible for managing information risks. In small organisations, this might be part of a combined role. If the organisation appoints an IG Lead who is not part of the senior management team or board, then there should be a SIRO who they report to at the highest level of the organisation. Organisations operating under the standard NHS contract are required to assign the role of SIRO.
Special Category Data	Data pertaining to an identified or identifiable individual that reveals their racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Term	Definition
Supporting Families	Supporting Families is part of a national programme that helps thousands of families across England to get the help they need to address multiple disadvantages through a whole-family approach, delivered by keyworkers, working for local authorities and their partners.
UK Data Protection Legislation	For the purpose of this template/guidance the UK data protection legislation means the UK GDPR and the DPA 2018 and regulations made under the DPA 2018 which apply to a party relating to the use of personal data.
UK General Data Protection Regulation (GDPR)	Legislation that determines lawful and unlawful use of individuals' data, and places requirements on those processing data, to ensure appropriate use and adequate protections.

## Appendix A Escalation Process

---

There may be times when there are professional disagreements around sharing of information to prevent crime and disorder. Initial attempts should be taken to resolve the problem between practitioners. If the disagreement is not resolved professionals should contact their supervisor/line manager/ team manager. It is then the responsibility of the supervisor/line manager/team manager to discuss the concerns with the equivalent supervisor/line manager/team manager in the other agency and take steps to resolve the issue.

If the problem is not resolved the supervisor/line manager/team manager should report to their senior manager. They will liaise with the equivalent representative in the other organisation who will attempt to resolve the professional differences.

This process of escalation will continue up to Executive Director level as necessary to resolve the issue.