



Overarching Tier 1

Keeping Bristol Safe Partnership's Children Safeguarding, Adult Safeguarding and Community Safety

Information and Data Sharing Agreement (DSA)

For multi-agency partnerships working together to safeguard children and adults and preventing crime and disorder in Bristol.

1 Introduction

To make informed decisions about safeguarding, prevent crime and disorder and achieve quality outcomes for individuals, we must share information with our partner agencies who also have responsibilities for safeguarding and prevention.

It has been frequently recognised in local and national reviews of practice that failing to share information at critical times has costs lives or led to detrimental outcomes. A fear of sharing sensitive information must not be a blocker to safeguarding and promoting the welfare of children, families and adults at risk or preventing crime and disorder. The relevant UK government departments and independent non-departmental government bodies responsible for protecting children and adults, preventing crime and disorder and/or regulating data protection therefore set out policy, legislation, and statutory guidance on how the protection system should work and data protection compliance is achieved at the same time. Those pieces of legislation are in place for the relevant sharing partners to be used to justify information sharing and to allow it in a safe and legal way. Some legislation puts a duty on organisations to share and others provide with them the power to do so. Information and Data are used interchangeably in this agreement.

The partners of this agreement are aware and understand their legal responsibilities to deliver safeguarding and prevent crime and disorder to the whole population as defined (amongst others) in the:

Children Act 2004, Section 10

Each local authority must make arrangements to promote co-operation between partners (including the ICB, Police, Schools and other) to improve the well-being of children including:

- (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.

Care Act 2014, Section 1

Safeguarding and Community Safety DSA

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);
- (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.

Crime and Disorder Act 1998

Duty on 'specified authorities' (Police, Probation, Fire, Health and Local Authorities) to prevent crime and disorder (including Anti-Social Behaviour) by:

- (a) Forming Community Safety Partnerships (CSP) with Police, Probation, Fire, Health and Local Authorities and any other organisations identified by the specified authorities. (s5)
- (b) Requiring creation and implementation of strategies to reduce crime and disorder. (s6)
- (c) Requiring consideration of crime and disorder implications when exercising their functions. (s17)
- (d) Providing an ability to share information for the purpose of preventing crime and disorder. (s115)

The effective and timely sharing of information between agencies and organisations is essential to enable early intervention and preventative work for safeguarding and promoting welfare of those experiencing and at risk of abuse and harm, for wider public protection and to reduce crime and disorder. For this reason, this Tier 1 DSA applies to all areas of adult and children's safeguarding and the prevention of crime and disorder. In the context of this document a Tier 1 DSA can be understood as an overarching, strategic agreement between Safeguarding partners defining the appropriate arrangements to support multi-organisational information sharing for safeguarding and crime and disorder prevention reasons, see appendix 1 for further details.

The UK GDPR sets out seven key principles which should lie at the heart of the partnership's approach to processing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation

Safeguarding and Community Safety DSA

- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Please visit the [ICO website](#) for more detail on the principles.

2 Contents

- 1 Introduction
- 2 Contents
- 3 Administration
- 4 Scope
- 5 Purpose and benefits
- 6 Responsibilities / partner commitments
- 7 Lawfulness
- 8 Guidance
- 9 Security Standards
- 10 Proportionality and necessity
- 11 Retention
- 12 Individual's rights
- 13 Transparency
- 14 Staff development
- 15 Incident management and complaints
- 16 Common sharing initiatives/area of work
- 17 Dissemination, monitoring, and review of the agreement
- 18 Signatories
- Appendix 1 – Glossary of terms
- Appendix 2 – Information sharing checklist
- Appendix 3 – Applicable Legislation
- Appendix 4 – Joint Resources
- Appendix 5 – Partners to this Agreement

3 Administration

The organisations below are signatories to this Tier 1 Data Sharing Agreement (see Appendix 5 for further details):

Organisation(s)
Bristol City Council
Avon and Somerset Police
NHS BNSSG Integrated Care Board (ICB)
Probation Service
Avon Fire and Rescue Service

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

Safeguarding and Community Safety DSA

General:

Date Tier 1 DSA comes into force:	20/12/2024
Last review:	
Date for review of DSA:	20/12/2025 (12 months from last review date)
DSA Owner (Organisation):	Bristol City Council
DSA Author(s):	Kevin Pointer, SCW Becky Lewis, Bristol City Council

Version control:

Version	Date	Author	Edit/Update
V0.1 Draft	30/01/2024	Antje Carpenter	First draft for consideration
V0.2 Draft	04/06/2024	Kevin Pointer	Draft amended following comments from working group
V0.3 Draft	16/09/2024	Lizzie Lambrou	Final proofreading edits
V0.4 Final	16/10/2024	Lizzie Lambrou	Finalising of document ready for signatures from statutory partners; full list of signatories to be stored separately by the Business Unit
V0.4 Final	12/11/2024	Lizzie Lambrou	Addition to section 6 - statutory agencies to have their own security standards

4 Scope

This Tier 1 Data Sharing Agreement applies to organisations operating in Bristol. It is a multi-agency agreement between Local Authorities, NHS Organisations, Police, Probation, Prison Service and Voluntary Sector Organisations. A full list of signatory organisations can be found under section 3 Administration and in appendix 5. The Agreement covers the sharing of personal and special category data about children, young people and adults for safeguarding and crime and disorder prevention reasons.

The Keeping Bristol Safe Partnership is constituted to deliver relevant statutory duties as follows:

- To safeguard and promote the welfare of children as required by The Children Act 2004 and supported by the statutory guidance, Working Together to Safeguard Children 2023
- To help and protect adults with care and support needs at risk of abuse or neglect as defined by the Care Act 2014 and supporting statutory guidance
- To reduce crime and disorder, substance misuse and re-offending as required by the Crime and Disorder Act 1998
- To cooperate to improve the wellbeing of children and young people as defined in The Children Act 2004
- To fulfil the responsibilities of the local partnership board as defined in the Domestic Abuse Act
- To cooperate to reduce Serious Violence in Bristol as defined in the Serious Violence Duty in accordance with the Police, Crime, Sentencing and Courts 2022

This Information and Data Sharing Agreement is designed to facilitate the multi-agency partnership to effectively fulfil these responsibilities in operational and strategic delivery.

The statutory members of the partnership consist of Bristol City Council, BNSSG Integrated Care Board, Avon and Somerset Police, Probation Service, Avon Fire and Rescue. The group is also represented by other members from health, education, and the voluntary and community sector.

Safeguarding and Community Safety DSA

This DSA is for use by professionals, staff and volunteers of organisations who have signed, and therefore agreed to the terms of this agreement and providers of services commissioned by the organisations who have signed this agreement. Safeguarding and preventing crime and disorder is everyone's responsibility, not just safeguarding or community safety practitioners.

Where there needs to be a more specific agreement about sharing data and/or information, it will be necessary to complete a Tier 2 information sharing agreement. This agreement should not be seen as an alternative to a Tier 1 agreement, Tier 2 agreements must be completed for specific information sharing projects between the partner organisations but will be linked to this overarching agreement. The Tier 2 agreement should be developed in line with best practice and/or using the National Template and Guidance provided by the Department for Education which can be found here ([Data Sharing Agreements – Important information for professionals \(somerset.gov.uk\)](https://www.somerset.gov.uk/data-sharing-agreements)).

The Care Quality Commission (CQC) describes safeguarding as protecting people's health, wellbeing, and human rights, and enabling them to live free from harm, abuse and neglect. It's fundamental to high-quality health and social care.

The Department for Health and Social Care provides guidance on the Care Act 2014 through the 'Care and support statutory guidance' and describes adult safeguarding as 'an adult's right to live in safety, free from abuse and neglect. It is about people and organisations working together to prevent and stop both the risk and experience of abuse or neglect...'.

The Care Act 2014 states that safeguarding duties apply to an adult aged over 18 who:

- d) has needs for care and support (whether or not the authority is meeting any of those needs) and
- e) is experiencing, or is at risk of, abuse or neglect, and
- f) as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

The Department for Education defines children's safeguarding as follows within their 'Working Together to Safeguard Children' guide to inter-agency working to safeguard and promote the welfare of children:

- a) providing help and support to meet the needs of children as soon as problems emerge
- a) protecting children from maltreatment, whether that is within or outside the home, including online
- b) preventing impairment of children's mental and physical health or development
- c) ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- d) promoting the upbringing of children with their birth parents, or otherwise their family network through a kinship care arrangement, whenever possible and where this is in the best interests of the children

Safeguarding and Community Safety DSA

- e) taking action to enable all children to have the best outcomes in line with the outcomes set out in the Children's Social Care National Framework.

The Information Commissioner's Office (ICO) recognises in their 10-step guide to sharing information to safeguard children that there is no single definition of safeguarding but highlights the inclusion of

- a. preventing harm;
- b. promoting the welfare of a child; and
- c. identifying risk in order to prevent harm (especially helpful where the risk may not be obvious to a single person or organisation).

Safeguarding must therefore be seen as a protection of wellbeing (including physical, mental & emotional); a prevention of harm and reduction of risk through care and support requiring information sharing. This allows intervention in immediate situations demanding the safeguarding of children and adults but also sharing for prevention and early intervention in less immediate or high-risk situations.

Information sharing with non-statutory agencies e.g. charities is within the scope of this Tier 1 DSA. There are a number of charitable organisations that offer support and services. Such organisations are not created under statute and therefore do not have statutory powers; nevertheless, they are often able to offer help and assistance in the form of counselling, advice, early help support, prevention and guidance as well as referring individuals to other organisations and charities within their network.

Adults in custodial settings are outside of the scope of this agreement e.g., prisons and similar approved premises. Prison Services have responsibility under the common law duty of care to protect those in their custody. Local Authorities however have a duty to assist prison services on adult safeguarding matters.

5 Purpose and benefits

The purpose of this Tier 1 Safeguarding DSA is to facilitate the lawful sharing, use and security of personal, special category data and criminal offence data in order to safeguard adults and children who require safeguarding intervention, facilitate the statutory functions of the Adult Safeguarding Boards and Children's Safeguarding Partnerships and prevent crime and disorder. This agreement will function as the foundation to embed strong, effective multi-agency arrangements that are responsive to local circumstances and engage the right people. Signatories to this agreement must be engaged to work in a collaborative way to provide targeted support as appropriate. This approach will provide flexibility to enable joint identification of, and response to, existing and emerging needs, and to agree priorities to improve outcomes. This agreement provides an overall framework for the secure sharing of information between the organisations (multi-agency/integrated working) that are parties to this agreement with the intention of:

- Protecting people's health, wellbeing, and human rights, and enabling them to live free from harm, abuse and neglect (including self-neglect).
- Taking action to enable all children and adults to have the best outcomes.
- Identifying risk and emerging threats in order to prevent harm (prevention, early intervention).
- Raising public awareness so that communities as a whole, alongside professionals, play their part in preventing, identifying and responding to abuse and neglect and promoting the welfare of children and adults.
- Preventing impairment of children's mental and physical health or development.
- Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care.
- Safeguarding adults in a way that supports them in making choices and having control about how they want to live.
- Providing information and support in accessible ways to help people understand the different types of abuse, how to stay safe and what to do to raise a concern about the safety or well-being of an adult.

Safeguarding and Community Safety DSA

- Collaborating, sharing and co-owning the vision for how to achieve improved outcomes for vulnerable people.
- Challenging appropriately and holding one another to account effectively.
- Sharing information effectively to facilitate more accurate and timely decision making.
- Ensuring that shared learning is promoted and embedded in a way that local services can become more reflective and that changes to practice are implemented.
- Reducing the need for individuals to provide duplicate information when receiving an integrated service.
- Managing risks, performance, service planning and auditing
- Preventing crime and disorder.

6 Responsibilities / partner commitments

By becoming a partner to this sharing agreement all organisations are making the following commitments. It is understood that signatories to this agreement are committing their whole organisation to entirely support the principles and carry out their responsibilities to the full.

Area of responsibility:

The parties to this DSA are committed to ensuring that information is shared appropriately between those professionals/organisations working with children, young people, and adults at risk of harm and/or involved in crime and disorder across Bristol and who have a legitimate need for that information to assist with delivering a high quality, integrated safeguarding and crime and disorder reduction service that meets the needs of the relevant individuals.

Organisations signed up to this agreement commit to sharing confidential information in accordance with their legal, statutory, and common law duties and meet the requirements of any additional supporting guidance.

All organisations must have in place policies and procedures to meet the national requirements for Data Protection, and which are consistent with this DSA. The existence of, and adherence to, such policies provide all organisations with confidence that data shared will be transferred, received, used, held and disposed of appropriately.

Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of personal information from other organisations, employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that data is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures; any proposed subsequent re-use of data which is sourced from another organisation should be approved by the source organisation.

Where processing is likely to result in a high risk to the rights and freedoms of a natural person (as per UK GDPR, Article 35), a Data Protection Impact Assessment will need to be completed and shared with the relevant partners as appropriate. This agreement does not replace the need to conduct a Data Protection Impact Assessment of the information or processes involved.

An individual's personal information must be complete and up to date and will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes, data should be anonymised.

Safeguarding and Community Safety DSA

Area of responsibility:
Where it is agreed that the sharing of personal information is necessary, only that which is needed, relevant and appropriate will be shared and would only be on a 'need to know' basis.
When disclosing information about an individual; organisations will clearly state whether the information being shared is fact, opinion, or a combination of the two.
There will be occasions where it is legal and / or necessary for organisations to request that personal information supplied by them is kept confidential from the person concerned. Decisions of this kind will only be taken on statutory grounds and must be linked to a detrimental effect on the physical or mental wellbeing of that individual or other parties involved with that individual. The outcome of such requests and the reasons for taking such decisions will be recorded.
All organisations agree to make reasonable efforts to ensure that recipients of personal information are kept informed of any changes to the information that they have received, so that records can be kept up to date, including this data sharing arrangement in their Privacy Notice
Careful consideration will be given to the disclosure of personal information concerning a deceased person, and if necessary, further advice should be sought before such data is released.
All organisations will ensure that Subject Access Requests and other Individuals' Rights requests made to them are responded to in accordance with the requirements outlined in the Data Protection Act (2018).
All organisations agree that appropriate training will be given to staff so that they are aware of their responsibilities to ensure personal information is processed lawfully.
All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.
Organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of personal information.
Extreme care and careful consideration should be taken where the disclosure of information includes third party information and particularly personal data relating to witnesses, victims or complainants.
The person or persons to whom a request is made must comply with such a request in relation to a child death review or child safeguarding practice review and if they do not do so, the safeguarding partners may take legal action against them.

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 ([Data Security and Protection Toolkit \(dsptoolkit.nhs.uk\)](https://dsptoolkit.nhs.uk)). If 'standards met' has not been achieved (organisation failed, not required to complete the DSPT, DSPT expired) organisations will be asked to confirm their plans (including the completion of the DSPT voluntarily) and share the relevant details. The statutory partners will consider the position of the organisation and make recommendations regarding the signing of the agreement. This will include statutory agencies which have their own security standards (such as police).

7 Lawfulness

Partners agree that in order to share personal data, there needs to be a relevant legal gateway. It is important to note that the existence of this Tier 1 Safeguarding Data Sharing Agreement does not provide partners with a legal gateway or secure an automatic right or obligation to share information with or from another partner. This may come from statute, common law, or legal precedent. Statutory powers (also referred to as legal gateways) will differ between the signatory organisations and cannot be prescribed in this Agreement. A list of commonly used legal gateways / applicable legislation for safeguarding and preventing crime and disorder sharing can be found in **Appendix 3**.

Principle legislation governing the protection and use of personal information is:

- a. UK General Data Protection Regulation (GDPR) 2016
- b. Data Protection Act (DPA) 2018
- c. Human Rights Act 1998 (article 8)
- d. The Common Law Duty of Confidentiality

Each signatory must be able to identify their lawful basis to share personal data which should be recorded within a Tier 2 Data Sharing Agreement.

The signatories of this agreement understand that *‘Consent is one lawful basis, but it is not required for sharing information in a safeguarding context. In fact, in most safeguarding scenarios you will be able to find a more appropriate lawful basis.’* This also applies to preventing crime and disorder scenarios. The most common lawful bases suitable for safeguarding and preventing crime and disorder purposes are public task, legitimate interests and legal obligation. ([Source ICO](#)) The UK GDPR provides several bases for sharing personal information. Partners will however be transparent with individuals whose data is being processed if it does not increase the risk of harm. ‘Engage, explain and cooperation’ with individuals supports the transparency of this sharing. The difference between consent to treatment/service opt-in and consent to share information under Data Protection laws must be understood by all partners to this

Safeguarding and Community Safety DSA

agreement. If consent to share information is considered to be required, this must be escalated to the relevant partner organisation's DPO for review.

8 Guidance

Partners will rely on the following guidance to adhere to principles defined in this agreement.

National Guidance:

Children:

- [Working together to safeguard children 2023](#) (Department for Education)
- [Information sharing advice for safeguarding practitioners](#) (Department for Education)
- [10 step guide to sharing information to safeguard children](#) (Information Commissioner's Office)

Adults & Children:

- [MAPPA Guidance](#) (Ministry of Justice, National Offender Management Service, HM Prison Service)
- [The Caldicott Principles](#) (National Data Guardian)
- [Serious Violence Duty](#) (Home Office)

Adults:

- [Care and support statutory guidance](#) (Department of Health and Social Care)
- [Practice guidance on sharing adult safeguarding information](#) (Social Care Institute for Excellence)
- [Deprivation of liberty safeguards](#) (Department of Health and Social Care)
- [Mental Capacity Act](#) (Act of Parliament)

Preventing Crime and Disorder

- [Information sharing for community safety - GOV.UK \(www.gov.uk\)](#)

Safeguarding and Community Safety DSA

- [Crime and Disorder Act 1998 \(legislation.gov.uk\)](https://www.legislation.gov.uk)

Local Guidance

:

- [South West Child Protection Procedures](#)
- [Keeping Bristol Safe Partnership Policy and Guidance](#)

9 Security Standards

Each partner will be responsible for ensuring data is subject to sufficient security.

All partners signed up to this agreement must ensure appropriate organisational policies and procedures are in place to cover the security of personal information under this agreement.

All reasonable steps should be taken to ensure that confidentiality of data is maintained, the integrity of data is preserved, and that data remains available where needed.

Controllers must also consider determining how they will test/audit the effectiveness of information security controls as part of a Data Protection Impact Assessment.

Sharing arrangements involving shared systems/assets will require joint decisions on security controls, therefore responsibility may be shared (pertinent to joint controller arrangements). This may include (but is not limited to) decisions on:

- A satisfactory level of compliance with industry cyber/information security standards (e.g. Cyber Essentials)
- A role-based access model
- Patching schedules
- Remote access solutions
- Third party security assurances and contractual arrangements (which may permit certain autonomy to maintain security)
- Recovery point/time objectives

A system level security policy should be developed jointly for such assets to document the agreed security controls/assurances for the sharing partners and demonstrate controller responsibility.

Appropriate contractual, data processing and confidentiality agreements must be in place to underpin the processing of personal information by a third party / processor.

10 Proportionality and necessity

The data relevant under this Tier 1 Data Sharing Agreement can include personal data, special category data and criminal offence data shared for the reasons of safeguarding and preventing crime and disorder.

Partners agree that only information that is relevant to the purposes should be shared with those partners who need it (need to know basis). Assessing proportionality and necessity for any sharing initiative under this agreement is paramount and should be documented to assure compliance with current UK data protection legislation. In circumstances where data is to be shared for safeguarding and preventing crime and disorder purposes both the benefits and the risks must be balanced against each other to assure the right level of proportionality and necessity. Organisations signed up to this Tier 1 Data Sharing Agreement must therefore include Caldicott Guardians (for Health), Service Leads or other equivalent individuals as they must be core to such decision-making. It is recommended under this agreement that organisations take a default 'starting position' of considering what data/information is reasonably, foreseeably needed. Data minimisation and proportionality will be maintained by only asking for data that is needed to fulfil a specified purpose.

Partners must consider any harm or detriment that may come from sharing information, and make sure this does not outweigh what is trying to be achieved (least intrusive amount of personal information to be shared appropriate to the risk presented). This is particularly important for sensitive information. Partners will consider who could be affected by any disclosures contemplating that sharing information about one individual may also have an effect on the privacy rights of others. Information must be of the right quality to ensure that it can be understood and relied upon.

Organisations signed up to this agreement will consider the level of identification required for each sharing initiative.

11 Retention

Records will be retained and disposed of in accordance with data protection legislation and national and local/organisational guidelines. Each organisation which has received information referred to in this agreement has to follow their own Retention and Disposal Policy which should state how long they will keep different types of information. Additionally, organisations should consider the business need beyond any national/industry code or guidance which could justify a shorter or longer retention period. Retention periods should be agreed with sharing partners, at the early stages of data sharing, in a Tier 2 Data Sharing Agreements as relevant (documented justification). Especially sharing arrangements involving shared systems/assets require joint decisions on retention and/or system configuration as they are more complex.

Health and Social Care partners will consider the NHS England Records Management Code of Practice to inform decision making (not applicable for children social care). Other partners will consult the relevant industry guidelines.

National inquiries must be considered when assessing records for destruction.

Any records which no longer need to be retained in accordance with the partners' own policies and procedures should be destroyed under secure conditions.

12 Individuals' Rights

The partners agree that in simple sharing arrangements each Controller will handle subject rights requests in accordance with their own established processes and policies. In multi-stakeholder sharing arrangements where shared information assets/systems are used, responsibilities for the handling of individuals' rights requests by the sharing partners must be clearly set out in the relevant Tier 2 Data Sharing Agreement. Requests relating to information shared for safeguarding purposes are likely to require careful consideration and may require assistance from partners as the provider of the information may be aware of a wider context to make a fully informed decision. Therefore, sharing partners agree to set out clear arrangements in a Tier 2 Data Sharing Agreement or Policy for the handling of individuals' rights and provide reasonable assistance to sharing partners as required.

The right to be informed – Partners must ensure that individuals are informed about the collection and use of their personal data and are provided with the privacy information required as per current data protection law. See the following section 'Transparency' for further detail.

The right of access – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate requests, what the process shall be if a request is received by them but is relevant to another organisation, how partners' involvement affects what they should disclose and the process for determining lawful reasons to withhold data from disclosure (i.e. if they are viewing data in a shared asset but are not controller nor a joint controller of the data, or if they are a joint controller).

The right to object and the right to restrict – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate objections and restriction requests, what the process shall be if an objection or restriction request is received by them but is relevant to another organisation and the process for determining whether to uphold the objection or restriction request (although unlikely due to the nature of processing).

The right to rectification – Sharing partners will agree a process of how to respond to requests for rectification (i.e. if received by them but it is relevant to another organisation). The process will be dependent upon the sharing arrangement; this may require action from multiple partners (especially when a request for rectification of a professional opinion is received) or by a single partner that has provided the data into a shared asset and may require partners to assist each other to determine whether data should be rectified.

The right to erasure - Sharing partners will agree a process of how to respond to requests for erasure (i.e. if received by them but it is relevant to another organisation). It is unlikely to uphold a request for erasure when processing for Safeguarding reasons.

Automated decision-making and profiling – If the sharing arrangement is to involve automated decision-making or profiling then the sharing partners will agree how individuals affected will be informed of this (unless an exemption applies) and how requests for a member of staff to review any such activity will be handled. As it stands, data used for safeguarding purposes is unlikely to be classed as ‘automated decision making’ or ‘profiling’ without human intervention prior to decisions being made that affect individuals.

The right to data portability – If the sharing arrangement is to involve the processing of data based on the explicit consent of the data subject or a contract with the data subject (which are both highly unlikely for the purposes of safeguarding), or data will be carried out by automated means, then the sharing partners shall ensure that it is possible for data to be provided to the data subject in a structured, commonly used and machine-readable format and/or have this data transmitted to another controller. The lawful basis of processing data for safeguarding purposes is not likely to be explicit consent. Therefore, it is unlikely that the right to data portability applies.

Most information rights requests will be dealt with by specific agencies who are the data controller of that information. In the event that an individual makes an information rights request in relation to information or data held by the Keeping Bristol Safe Partnership e.g. in respect of data reports, quality assurance or statutory reviews, then the request should be sent to the Keeping Bristol Safe Partnership Business Unit at kbsp@bristol.gov.uk to coordinate the appropriate response. When a partner agency requires cooperation from the wider partnership to respond to a Subject Access Request, they can contact the Keeping Bristol Safe Partnership Business and Partnership Manager to ensure appropriate liaison if they have been unable to progress this within their existing processes. The Keeping Bristol Safe Partnership Business unit is able to access advice and guidance from Bristol City Council’s Data Protection Officer.

13 Transparency

Each organisation must be clear, open and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'. The sharing partners (controllers) each have a responsibility to take reasonable steps to ensure that individuals (to whom data they are processing pertains) are informed of the uses of their data. The sharing partners will therefore agree an approach to informing individuals about the sharing of data for safeguarding purposes. This may, for example, take the form of each partner updating their own privacy information (i.e., a website privacy notice) or the partners may agree to reference a single privacy notice from their own privacy information, which is then maintained by one or several organisations (e.g., joint controllers). The privacy information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language, tailored to children if required.

Best practice in respect of transparency is to take a layered approach by utilising various methods to communicate information about how individuals' data is being used, i.e., website privacy notice, leaflets, posters, letters, conversations, etc., However, given the nature of processing for safeguarding and preventing crime and disorder purposes it may not always be appropriate. The sharing partners must consider exemptions (e.g., law enforcement purposes under Part 3 of the DPA 2018, or serious harm to the physical or mental health of any individual).

14 Staff development

Each sharing partner must ensure that its staff are sufficiently trained to handle personal data appropriately as part of their controller responsibilities under UK data protection law (the UK GDPR principle of 'accountability' and specifically principle 5(f) (integrity and confidentiality) as an appropriate organisational measure). This can include training on confidentiality, data protection, record keeping, records management, system training, as well as more specific training on handling individuals' rights requests for those staff typically involved in these, etc. Sharing partners should therefore consider whether staff affected by a new sharing arrangement will require additional training (in addition, controllers should continually assess the training needs of their workforce, which is often done by maintaining/appraising a 'Training Need Analysis' on a routine basis).

All staff must have access to the policies of their own organisation, this agreement and any materials jointly developed. For the purposes of this agreement the supporting processes will be that all staff authorised to access information will be trained in the basic requirements of the Data Protection legislation and have an awareness of the implications associated with shared information. They will also understand the risks associated with inappropriate disclosures and the impact that this has on safeguarding and the necessity to undertake thorough checks. Staff contracts must therefore contain appropriate confidentiality clauses detailing the possible consequences of unauthorised or inappropriate disclosure of personal information. Each organisation must have in place disciplinary procedures to be invoked if a member of staff is found to have breached the confidentiality of an individual. Consideration should be given to the category and nature of information to which staff have access and whether their role includes any specific requirements to access personal information.

The process of supervision is generally confidential between the supervisor and supervisee(s). The ground rules in relation to confidentiality will be made explicit, such as ownership of supervision records, retention of information. There may be occasions when it is necessary to share information with other practitioners/ managers/ external agencies/professional bodies in the best interests of the child/adult at risk in line with organisational and multi-organisational information sharing agreements. Poor or dangerous practice will be addressed in line with partner organisation policy and procedures.

The partners of this agreement will work together to jointly develop staff training materials to allow organisations to this agreement to incorporate the principles of this agreement. Resources can be found in appendix 4.

15 Incident Management and Complaints

Data security and protection incidents must be treated with priority and urgency; swift action should be taken to contain incidents and prevent both the number of individuals that may be affected and increased severity for those already affected. As such, sharing partners must inform the responsible controller as soon as possible (where they become aware of an incident that they are not responsible for or are only partially responsible for). Sharing partners must also determine whether other sharing partners (beyond those responsible) should be informed as concerns may have been, or be, raised to them that are linked to the incident, which they may otherwise not know.

Given the nature of the data involved in processing for safeguarding and preventing crime and disorder purposes, care and consideration should be given to who needs to be informed of an incident (in terms of both sharing partners, as well as the individuals affected (duty of candour) and/or third parties).

Where an incident is isolated and deemed to only affect one sharing partner than the incident may be handled solely by that sharing partner according to their own incident management policy and processes. Where multiple sharing partners are affected, they must be prepared to establish a joint incident response plan. Clear responsibilities should be set out for any joint controller arrangements.

Complaint handling should follow a similar path; however, they are unlikely to require such priority/urgency unless they are intrinsically linked to an incident.

All partner organisations must put in place processes that allow concerns about non-compliance with this agreement to be reported to the designated person.

16 Common sharing initiatives / area of work

The below sharing initiatives are covered by this agreement and give detail of how data is being used to safeguard children and adults and prevent crime and disorder. Partners share information to contribute to:

Child Death Overview Panel (CDOP) - Children

The Child Death Overview Panel (CDOP) is a group of multi-agency professionals who meet ten times a year to carry out an independent review of deaths of children in their area. The purpose of the panel is to learn lessons and share any findings which may help to prevent future deaths. The panel will consider and identify any issues relating to the death which may be relevant to the welfare of children in that area or to public health and safety. They will consider if action should be taken in relation to the issues identified to help try to prevent similar deaths happening again in the future. For the panel to investigate a child's death essential information needs to be gathered including demographic data, and information relating to the circumstances of death and background medical history. Whilst not all deaths reported to the coroner proceed to inquest (although most unexplained deaths of children do) there is also a duty on professionals to disclose such information to the coroner in an un-redacted format and the coroner has their own common law and statutory powers to enforce such disclosure. For the purposes of KBSP we share information with the CDOP under Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject and Schedule 1 of the Data Protection Act 2018 Article 9(2)(g) Substantial Public Interest for statutory and government purposes, and for safeguarding of children and individuals at risk.

Child Death Reviews - Children

Multi-agency partners share information through the Joint Agency Review process (for unexpected deaths of children) and subsequent Child Death Review to learn from child deaths. Information is submitted through eCDOP and coordinated by the West of England Child Death Office. Partners provide information about their involvement with the child and their wider family and the child's death.

Child Safeguarding Practice Review - Children

The KBSP have a statutory responsibility to undertake rapid reviews and Local Child Safeguarding Practice Reviews (CSPRs) where abuse or neglect of a child is known or suspected, and the child has died or been seriously harmed. The purpose of a Child Safeguarding Practice Review is to establish whether there are lessons to be learnt from the case about the way in local professionals and organisations work together to safeguard and promote the welfare of children. Identify clearly what those lessons are, how they will be acted on, and what is expected to change as a result, and therefore, improve inter-agency working and better safeguard and promote the welfare of children. When undertaking a review or CSPR the KBSP collect and share personal information which includes the name, date of birth and addresses of individuals that are pertinent to the CSPR and request information and records from professionals who have worked with children and families including health records, social care files and criminal records. This information is shared with partners who are involved in review's learning panel and/or agencies' safeguarding leads. The information requests are centrally held and coordinated by the KBSP Business Unit. The information will be shared with an Independent Reviewer where they have been commissioned. The final reports will be shared with the National CSPR Panel, OFSTED and the Department of Education as well as other inspectorates where required such as the CQC and HMIC.

Section 17 (Children Act 1989)

Information is requested by agencies involved in working with children and their families where they are being assessed or are receiving a services as child in need. This is to enable the agencies to provide services which meet the children's identified needs in order to keep them safe from neglect or physical, emotional or mental harm, or to protect their physical, mental, or emotional well-being. Information will be shared verbally between professionals in meetings and communication, in writing and through automated information sharing systems such as Think Family Database, CPIS and Connecting Care.

Section 47 (Children Act 1989)

Children's social care have a duty under Section 47 of the Act to make enquiries where there is reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm. These enquiries may be undertaken as a single agency or jointly with police and/or health professionals. Children's social care will seek relevant information from other professionals about the child, their wider family, and/or individuals who may pose a risk to them or be responsible for their care. Information will be provided through strategy meetings, in verbal and/or written communication, through observations and joint visits to children and families, and through automated information sharing electronic systems.

Child Protection Notifications

Agencies are required to check what information is held by other professionals in circumstances where this will support them to make a decision relevant to a child's safety. This includes requesting information from children's social care and/or the police in the event of probation; adoption and fostering agencies making registration decisions of new carers; children social care assessing urgent suitability of connected carers of children (eg reg 24 and private fostering); children in care moving out of area; pregnant women who may move across health authority areas where there is a risk to the unborn or the pregnant woman. This information should be sought from the relevant partner agency who holds it.

Multi Agency Safeguarding Hub (MASH) – Children and Adults

The goal of a MASH (Multi Agency Safeguarding Hub) is to improve safeguarding and promote the welfare of children and young people and adults through the timely exchange of proportionate and accurate information following an enquiry by any professional or member of the public. The MASH environment is unique in the way it enables multiple sources of information to be considered and shared in a secure and safe location. For Children information is referred to the First Response service and the MASH process is triggered. This assists decision making about the threshold of concern and what level of support is required from agencies.

Multi Agency Risk Assessment Conference (MARAC) – Children and Adults

A Multi Agency Risk Assessment Conference (MARAC) is a multi-agency meeting attended by agencies to discuss cases of domestic violence and abuse that professionals consider to be 'high risk'. The primary focus of the MARAC is to safeguard the adult victim and any children. The MARAC is coordinated by Avon and Somerset Police who compile, triage and store the MARAC referrals. Case lists and information are circulated by relevant MARAC partners by secure email. Additionally, the MARAC aims to make connections with other forums to safeguard children and manage the behaviour of the perpetrator. The working assumption of the MARAC is that no single agency or individual can see the complete picture of the life of a victim, but all may have insights that are crucial to their safety. KBSP partners will share information at MARAC meetings to ensure risk is managed and responded to effectively, and to reduce further harm.

Multi Agency Public Protection Arrangements (MAPPA) – Children and Adults

Multi-agency public protection arrangements (MAPPA) are in place to ensure the successful management of violent and sexual offenders. “MAPPA offender” is someone who satisfies the criteria set out in sections 325 and 327 of the Criminal Justice Act (2003) and is therefore liable to management under MAPPA. The Criminal Justice Act 2003 expressly permits information sharing between Responsible Authorities and Associate agencies for the purposes of assessing and managing the risks presented by MAPPA offenders under sections 325(4B) 325(4D) and (4E) of the CJA Act. Information sharing about MAPPA is coordinated by the Avon and Somerset Police MAPPA team. Information is shared with relevant professionals on the MAPPA Panel by email and through multi-agency meetings. The KBSP will also share information pertaining to MAPPA under Part 3 of the Data Protection Act 2018 which namely is for 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.

Safeguarding Adult Reviews (SAR)

A Safeguarding Adult Review (SAR) is a process conducted when an adult at risk has died or suffered serious harm, and there are concerns about the care or services they received. The KBSP conduct SARs in line with the Care Act (2014) and aims to identify areas for improvement in policies, procedures, and practice, and to inform training and development for professionals. In undertaking these we aim to prevent similar incidents in the future. Sharing the right information, at the right time, with the right people is fundamental to good practice in safeguarding adults. When undertaking a SAR the KBSP collect and share personal information which includes the name, date of birth and addresses of individuals that are pertinent to the CSPR and request information and records from professionals who have worked with adults including health records, social care files and criminal records. This information is shared with partners who are involved in review’s learning panel and/or agencies’ safeguarding leads. The information requests are centrally held and coordinated by the KBSP Business Unit. The information will be shared with an Independent Reviewer where they have been commissioned. The final reports will be shared with relevant partners and published.

Domestic Abuse, Stalking, Harassment and Honour Based Violence (DASHH) - Adults

Information about survivors and perpetrators of domestic abuse, stalking, harassment and honour-based violence may be shared outside of MARAC between partners for the purpose of implementing risk management strategies to reduce the risk of abuse or death. Information may be shared by email, through referrals to services or within risk management meetings or discussions between partnership.

Domestic Homicide Reviews (DHR) - Adults

The KBSP have a statutory responsibility to undertake Domestic Homicide Reviews (DHRs). The purpose of a DHR is to establish whether there are lessons to be learnt from the case about the way in local professionals and organisations work together to protect a victim(s) from domestic abuse, identify clearly what those lessons are, how they will be acted on, and what is expected to change as a result, and therefore, improve inter-agency working and better safeguard and promote the welfare of children and adults. When undertaking a DHR the KBSP collect and share personal information which includes the name, date of birth and addresses of individuals that are pertinent to the CSPA and request information and records from professionals who have worked with families including health records, social care files and criminal records. This information is shared with partners who are involved in review's learning panel and/or agencies' safeguarding leads. The information requests are centrally held and coordinated by the KBSP Business Unit. The information will be shared with an Independent Reviewer where they have been commissioned. The final reports will be shared with the Home Office and published.

Prevent and Channel – Children and Adults

The Prevent programme is designed to help prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support, including through the multi-agency Channel programme. Referrals are made to the Avon and Somerset Police Prevent Team and Bristol City Council Prevent Coordinator. The team will triage the information, seek further relevant information where required to inform the agency assessment and store it securely on police and local authority systems. Where a Channel Panel threshold is met the individual's details will be shared with relevant agencies and will be discussed in a multi-agency meeting to agree a plan of support which will be regularly reviewed.

Prevention of Serious Violence and Safeguarding from Exploitation – Children and Adults

Safeguarding and Community Safety DSA

Information to prevent serious violence and safeguard children from exploitation will be shared by partners through: Avon and Somerset Police reporting and intelligence portals; referrals to children's social care; intelligence reporting to the Safer Options Hub; Hospital knife injury pathway and through to specialist exploitation service run by Barnardo's. Intelligence will be collated and shared through Safer Options meetings, child protection strategy meetings, risk management meetings, daily triage meetings, Operation Topaz briefings, community response meetings, community safety meetings, police tasking meetings and contextual safeguarding meetings. Intelligence will also be collated from multi-agency risk management flagging systems, Think Family database products and police intelligence systems and shared with relevant professional groups. These will ensure that intelligence and information is shared with relevant involvement professionals about individuals, places and groups of concern to enable the development of multi-agency plans to reduce the factors contributing to the risk of violence and exploitation. All agencies will be first responders for modern slavery making relevant referrals to the National Referral Mechanism.

Section 42 of the Care Act – Adults

Organisations share information with each other to:

- prevent death or serious harm
- coordinate effective and efficient responses
- enable early interventions to prevent the escalation of risk
- prevent abuse and harm that may increase the need for care and support
- reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
- identify low-level concerns that may reveal people at risk of abuse
- protect adults with care and support needs from organisations and people in positives of trust
- help people to access the right kind of support to reduce risk and promote wellbeing
- help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- reduce risk of organisational abuse or neglect

This will be done primarily through referrals to the adult safeguarding teams who will coordinate information sharing across the multi-agency partnership through telephone calls, emails and multi-agency meetings.

Anti-Social Behaviour

Anti-Social Behaviour is addressed through an incremental partnership approach that emphasises identification of underlying factors causing ASB and then leveraging in relevant interventions to address those factors. This work is done on a reactive basis (commonly in response to reports) and a data-led proactive basis where the partnership looks to identify repeat victims, perpetrators and geographic hotspots and carries out problem solving activity to address them. Information is shared by partners through the police and local authority anti-social behaviour teams.

Hate Crime

Information about victims and perpetrators of Hate Crime are shared through police reporting systems, adult and child safeguarding referrals, referrals to the Bristol Hate Crime services and the anti-social behaviour team. These services then take steps to implement single and multi-agency action plans to respond to and reduce the harm. This work is done on a reactive basis (commonly in response to reports) and a data-led proactive basis where the partnership looks to identify repeat victims, perpetrators and geographic hotspots and carries out problem solving activity to address them and ensure victims are adequately supported.

Community Safety Partnership Needs Assessment/Plan

It is a statutory duty for the Community Safety Partnership (CSP) to carry out a community safety needs assessment that is used to inform the CSP plan. In order to fulfil this requirement, there is a need to share anonymised data amongst the partners.

KBSP Quality Assurance, Inspection and Scrutiny

The KBSP has a requirement to quality assure the effectiveness of safeguarding and community safety arrangements. To do this the KBSP Business Unit will coordinate the sharing of information in the form of reports, data, audit reports and peer reviews and inspections to enable the analysis of quality and performance of systems. This will include sharing personal information of individuals particularly in the case of quality assurance activity. Where this is the case a specific review team will undertake assurance of that area

Safeguarding and Community Safety DSA

of practice. Steps will be taken to ensure that personalised information is protected in the sharing of learning for example in learning reports or in the KBSP's annual report.

LADO and allegations against professionals - children

The LADO (Local Authority Designated Officer) is a local authority role who is responsible for ensuring that children are protected from abuse and/or neglect by people in positions of trust (professionals and volunteers). The LADO provides advice and guidance to other professionals and helps determine how allegations should be investigated and managed. The LADO will receive information by email referral form. The LADO helps co-ordinate information sharing also monitors and tracks any investigation with the expectation that it is resolved as quickly as possible. The LADO will provide advice and guidance to organisations, regulators, inspectorates and individuals. They will review HR reports and investigations material which could include CCTV, body maps, statements from staff, observation charts. The LADO will provide anonymised data to the KBSP about the effectiveness of allegations management in the city.

Modern Slavery

The Modern Slavery Act requires some members of the KBSP to act as First Responder Organisations to share information in the identification and response to victims of modern slavery including referrals through the National Referral Mechanism. There is also a need to try and prevent this form of crime through multi-agency work, both joint casework (requiring information sharing on a personal level) and wider strategic partnership approach (likely to require anonymised data sets to be shared). This will include information sharing about potential perpetrators of modern slavery and trafficking.

It should be noted that the above list is not exhaustive but any data sharing for safeguarding children, safeguarding adults and preventing crime and disorder purposes will still fall under this agreement.

There is a duty on Local Authorities under the Children and Families Act 2014 and the Care Act 2014 to assure a safe transition from Children's to Adult Services. Where there are ongoing safeguarding concerns or needs for a young person and it is anticipated that on

Safeguarding and Community Safety DSA

reaching 18 years of age, they are likely to require adult safeguarding support, the relevant arrangements should be discussed as part of the transition and the appropriate information must be shared.

17 Dissemination, monitoring and review of the agreement

This protocol will be shared with all signatories, processors and relevant parties for the purpose of upholding the principles of this agreement.

It is intended that this overarching Tier 1 Data Sharing Agreement contains high level principles and partner commitments only. It will therefore be reviewed annually to establish if the sharing remains necessary, still operates as intended and, has or is, achieving the intended benefits, unless legislative changes or other significant changes require immediate action. The monitoring and review of this protocol will be undertaken by Keeping Bristol Safe Partnership Business Unit.

Subject to there being no significant changes, the agreement may be extended by a further five years without seeking further approval or new signatures. However, any significant changes will require the full approval process.

In the event that this Tier 1 Agreement is not renewed or is otherwise withdrawn, it is incumbent on the parties to amend their records accordingly and to communicate the status of the agreement within their respective organisations to interested parties and the wider public as necessary. The obligations of confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

18 Signatories

Each organisation should identify who is the most appropriate post holder within their agency to sign the DSA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their agency/organisation to the agreement. Additionally, each agency will be asked to identify the post which is responsible on a day-to-day basis for monitoring compliance with this DSA.

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

Name: Hugh Evans

Role: Caldicott Guardian and Executive Director Adults & Communities

Signature: 


Date signed: 05/12/2024

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: data.protection@bristol.gov.uk

2. Signed on behalf of: Bristol, North Somerset and South Gloucestershire ICB

Name: Dr Joanne Medhurst

Role: Caldicott Guardian

Signature: 

Date signed: 29/10/2024

Safeguarding and Community Safety DSA

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Bnssg.foi@nhs.net

3. Signed on behalf of: Avon Fire and Rescue Service

Name: Nikki Rice

Role: Vulnerable Adults Manager & Joint Safeguarding Lead

Signature: 

Date signed: 10/12/2024

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: DPO@avonfire.gov.uk or FOI-DP@avonfire.gov.uk

4. Signed on behalf of: Avon and Somerset Police

Name: Mark Runacres

Role: Superintendent, Bristol Police Commander

Signature: 

Date signed: 18/12/2024

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Dpo@avonandsomerset.police.uk

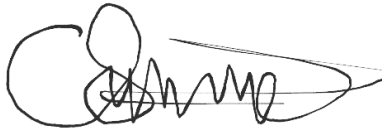
5. Signed on behalf of: Probation Service

Name: Claire Summers

Safeguarding and Community Safety DSA

Role: Head of Bristol & South Gloucestershire PDU

Signature:

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

Date signed: 18/12/2024

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Claire.Summers@justice.gov.uk

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

Appendix 1 - Glossary of terms

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: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf
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 one of three ways: 1. the service user has given consent for their information to be used; 2. the balance of public and private interest favours public interest disclosure; or 3. a statutory basis exists which permits or requires disclosure. (source: Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016, Explanatory Note, Common Law Duty of Confidentiality)
Consent	Consent under Data Protection Law is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Safeguarding and Community Safety DSA

Term	Definition
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.
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.
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).
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.

Safeguarding and Community Safety DSA

Term	Definition
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 here) 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 here).
Legal gateway	Legislation and common law that establishes justifiable grounds for the processing of personal data.
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).
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.
Privacy Notice	A privacy notice is a publicly available document that should identify who the data controller is, with contact details for its Data Protection Officer. It should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing.
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.
Secure File Transfer Protocol (SFTP)	A protocol for securely accessing and transferring large files across the web.

Safeguarding and Community Safety DSA

Term	Definition
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.
Tier 1 DSA	In this document Tier 1 Data Sharing Agreement can be understood as an overarching Multi Agency Safeguarding Data Sharing Agreement which can be used by all agencies and organisations within the relevant geographical area to provide a framework for data sharing between the partners. Sometimes Tier 1 Agreements are referred to as: Overarching DSA, Data Sharing Protocol, Data Sharing Charter, and others.
Tier 2 DSA	In this document a Tier 2 Data Sharing Agreement can be understood as a more operational document setting out the purpose of data sharing for a specific initiative, detailing what happens to the data at each stage, setting specific standards and helping all the parties involved in sharing to be clear about their roles and responsibilities.
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 2 - Information sharing reflective tool

By sharing information, we work better together, and this Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Data Sharing Agreement encourages the appropriate sharing of personal information between the relevant agencies. If you cannot identify an individual from the information you are planning to share, then you are free to share. However, if the information identifies someone, please use this tool to help you determine that it is safe to share information. Here is tool setting out what you will need to do to go from having concerns about sharing data to sharing data legally and securely with confidence.

Why is the information needed?

What is the purpose for sharing the relevant information, think about the purpose for individuals, your organisation and the wider public. Does it fulfil the purposes outlined in this Tier 1?

What information is needed?

Be specific and descriptive, consider how often it is required.

What organisation can provide the information?

Have you explored if the information is available already, maybe in other parts of your organisation. Have you spoken to a counterpart in the potential sharing organisation who can advise you on what information is available and how often.

Have you completed a Data Protection Impact Assessment (DPIA)?

Be aware that a DPIA is likely to be a legal requirement. Complete it before you start processing any data.

How will it be transferred?

Consider your options and assess the risk of those. Transfers must be safe and secure, consult with your technical teams for more complex digital solutions (e.g., data transfer system to system or via Secure File Transfer Protocol [SFTP]).

Where will it be held?

Consider your options and assess the risk of those. Any information must be held safe and secure, consult with your technical teams for more complex digital solutions.

Are you sure the information is accurate and not misleading?

Take all reasonable steps to ensure the personal data you hold is not incorrect or misleading. If you discover that personal data is

Safeguarding and Community Safety DSA

incorrect or misleading, you must take steps to correct or erase it as soon as possible. Carefully consider any challenges to the accuracy of personal data.

How will you process it?

Define what solutions are available to process the information (e.g., data warehouse, modelling, risk scoring, manual usage to inform cases), work closely with the relevant teams (e.g., analytics, IT, ethics).

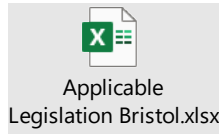
How long will you keep it?

Follow your internal retention policy and establish how long you need the information. Include any potential outcome products and long-term requirements to hold the data.

How will you delete the data?

Follow your internal records retention or data destruction policy to assure safe destruction of the information you hold. Consider the method depending on your storage solution to allow for safety of destruction.

Appendix 3 - Applicable Legislation



Appendix 4 – Joint Resources

Name of Document/Tool	Description	Source Organisation(s)
<i>e.g. Training material, fair processing notices, DSA & DPIA templates, policies, guidance etc.</i>	<i>e.g. Lawful Basis and Legal Framework document agreed by all statutory partners and shared with all non-statutory partners.</i>	<i>e.g. the content has been produced by the Police, Health Trust and the Local Authority, input from Barnardo's has been received and included.</i>

Appendix 5 – Partners to this agreement

Organisation	Address	ICO registration number	Contact person	Contact details
Bristol City Council	City Hall, College Green, Bristol, BS1 5TR	Z5873747	Ben Hewkin DPO	Data.protection@bristol.gov.uk
Avon and Somerset Constabulary	Valley Road Portishead Bristol BS20 8JJ	Z4882079	Kevin Coe – Information Governance Manager	Dpo@avonandsomerset.police.uk
NHS BNSSG Integrated Care Board (ICB)	100 Temple Street, Redcliffe, Bristol BS1 6AG	Zb344972	Caldicott Guardian	Bnssg.foi@nhs.net
Probation Service	102 Petty France London SW1H 9AJ	Z5679958	Claire Summers – Information Asset Custodian	claire.summers@justice.gov.uk
Avon Fire and Rescue Service	Police & Fire Headquarters PO Box 37 Valley Road Portishead Bristol BS20 8JJ	Z6748396	Lucy Jefferies DPO	DPO@avonfire.gov.uk or FOI-DP@avonfire.gov.uk

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