

Avon and Somerset Region Safeguarding Partnerships Overarching Tier 1 Information Sharing Agreement (ISA)

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement - for agencies and organisations safeguarding children, families and adults at risk or preventing crime and disorder across the Avon and Somerset region: Bath & North East Somerset, Bristol, North Somerset, Somerset and South Gloucestershire.

1 Introduction

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

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; and
- e) social and economic well-being.

Section 16E and 16LA: Places a duty on specified safeguarding partners (s16LA (4)) to make arrangements for the purpose of safeguarding and promoting the welfare of children in the area.

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;

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

- 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; and
- 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 ISA 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 ISA can be understood as an overarching, strategic agreement between Safeguarding partners defining the appropriate arrangements to support multi-agency 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.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

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

2 Version Control

Date Tier 1 ISA comes into force:	30/09/2026
Last review:	24/09/2026
Date for review of ISA:	24/09/2029
ISA Owner(s) (Organisation(s)):	Avon and Somerset Police, NHS BNSSG Integrated Care Board, Somerset & B&NES NHS Integrated Care Board, Bath & North East Somerset Council, Bristol City Council, North Somerset Council, Somerset Council, South Gloucestershire Council, Probation Service, Devon & Somerset Fire & Rescue Service, Avon Fire & Rescue Service
ISA Author(s):	Lucy Wilkins, Information Governance & Records Manager, Somerset Council Rebecca Leggett, Policy Manager, Somerset Safeguarding Children Partnership

Version	Date	Author	Edit/Update
V1.0	14/08/2025	-	Regional Child Safeguarding Partnership Group reviewed current local partnership ISAs and agreed to adopt a regional ISA approach using the DfE template
V1.0 Draft	20/08/2025	Lucy Wilkins SC IG / Rebecca Leggett SSCP	Draft Child Safeguarding T1 ISA submitted for consideration/accuracy by Regional LCSP Business Managers
V1.1 Draft	10/10/2025	Lucy Wilkins SC IG / Rebecca Leggett SSCP	Regional Partnership Business Managers requested T1 ISA update to incorporate Regional Safeguarding and Community Safety Partnerships
V1.2 Draft	10/12/2025	Lucy Wilkins SC IG / Rebecca Leggett SSCP	Updated draft submitted to regional Safeguarding and Community Safety Partnership Executives/Boards for feedback
V1.3 Draft	21/01/2026	-	Consultation with Regional Partnership Business Managers and partner Information Governance Leads for feedback. Collaborative meeting held 27/03/2026
V1.4 Draft	21/04/2026	Lucy Wilkins SC IG / Rebecca Leggett SSCP	Amended draft submitted for accuracy and consideration by Regional Group Business Managers and Partnership Executives/Boards for approval prior to signatures
V1.4.1 Draft	14/07/2026 14/09/2026	Lucy Wilkins SC IG / Rebecca Leggett SSCP	Strengthened against DfE Information Sharing Duty statutory guidance (sections 16E and 16LA of the Children Act 2004)
V1.5	15/09/2026	-	Document circulated to Authorised Signatories - Partners to this Agreement (see section 19)
V1.5.1	24/09/2026	Lucy Wilkins SC IG / Rebecca Leggett SSCP / Kevin Coe (A&SC)	Amended to reflect Avon and Somerset Police requests for the inclusion of joint ownership by all authorised signatories, enhanced security standards, strengthened handling instruction requirements, and additional provisions relating to data quality and accuracy obligations.
	30/09/2026		Ratification and publication

3 Contents

- 1 Introduction
- 2 Version Control
- 3 Contents
- 4 Purpose
- 5 Benefits
- 6 Scope
- 7 Responsibilities / partner commitments
- 8 Lawfulness
- 9 Law and Guidance
- 10 Security Standards
- 11 Proportionality and necessity
- 12 Data Quality
- 13 Retention
- 14 Individuals' Rights
- 15 Transparency
- 16 Staff Development
- 17 Incident management and complaints
- 18 Dissemination, monitoring, and review of the agreement
- 19 Signatories - Partners to this Agreement

Appendices:

- Appendix 1 – Common sharing initiatives / area of work
- Appendix 2 – Applicable Legislation
- Appendix 3 – Joint Resources
- Appendix 4 – Information sharing principles
- Appendix 5 – Collaborative Data Breach Process
- Appendix 6 – Minimum Security Standards
- Appendix 7 – Glossary of terms
- Appendix 8 – Information Governance Contacts

4 Purpose

The purpose of this Tier 1 Safeguarding ISA 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.
- 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.

It is important to note that processing of personal data is inevitable in these learning activities, however the focus of the learning activities is not on the individual, but on the systems and processes being adhered to so that good practice and improvements can be identified, and actions implemented. Learning activities require processing of personal data to achieve the purposes outlined above, whether these be prescriptive in law, or a duty that is placed as a result of legislation or statutory guidance.

This information sharing agreement aims to achieve a balance between the need to share personal information and special category data to fulfil the partnership functions, and not stifle the learning processes, whilst ensuring that information sharing is adequate, necessary and proportionate.

This Information Sharing Arrangement (ISA) provides the framework for sharing of personal data between agreed parties to meet the purpose of improving access to information in order that each organisation can fulfil their legal duties.

5 Benefits

Benefits of the sharing are:

- Preventing impairment of adults and 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.
- 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 quality assurance activities.

6 Scope

This Tier 1 Information Sharing Agreement covers the sharing of personal and special category data about children and adults for safeguarding reasons. The organisations that are signatories to this Tier 1 Information Sharing Agreement can be found in section 19 (Signatories - partners to this agreement).

This ISA 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 is everyone's responsibility, not just safeguarding practitioners.

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

The Department for Education defines children's safeguarding as follows within 'Working Together to Safeguard Children'¹ guide to inter-agency working to safeguard and promote the welfare of children:

- a. Protecting children from maltreatment
- b. Preventing impairment of children's mental and physical health or development
- c. Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
- d. Taking action to enable all children to have the best outcomes - set out in the Children's Social Care National Framework²:
 - Outcome 1: Children, young people and families stay together and get the help they need
 - Outcome 2: Children and young people are safe in and outside their homes
 - Outcome 3: Children and young people are supported by their family network
 - Outcome 4: Children in care and care leavers have stable, loving homes

This ISA covers the operation of section 16LA of the Children Act 2004 - [Information Sharing Duty Statutory guidance for safeguarding organisations and their practitioners](#): the sharing of information about a child, or any other individual connected to a child, whether an adult or another child, where it is relevant to safeguarding and promoting the welfare of that child.

The Information Commissioners 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).

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'³ 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 (section 42) states that safeguarding duties apply to an adult (aged over 18) who:

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

¹ [Working Together to Safeguard Children: A guide to multi-agency working to help, protect and promote the welfare of children](#) [March 2026, page 9]

² [Children's Social Care National Framework](#) These children's social care specific outcomes support and align with the Keeping Children Safe priority outcome in the Local Outcomes Framework that sets out key priority outcomes that are delivered at the local level and driven by councils as local leaders of place.

³ [Care and support statutory guidance - GOV.UK](#) [Sep 2025]

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 and organisations e.g., charities is within the scope of this Tier 1 ISA. There are a number of charitable organisations that offer support and services. Such organisations do not have statutory powers; nor are they subject to the same duties particularly under sections 16E and 16LA of the Children Act 2004; nevertheless, they are often able to offer help and assistance in the form of counselling, advice, support and guidance as well as referring individuals to other organisations and charities within their network.

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 2 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 at [Data Sharing Agreements – Important information for professionals \(somerset.gov.uk\)](https://www.somerset.gov.uk/data-sharing-agreements-important-information-for-professionals/)

7 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 entire organisation to entirely support the principles and carry out their responsibilities to the full.

Area of responsibility:

The parties to this ISA are committed to ensuring that information is shared appropriately between those professionals/organisations working with people at risk of harm who have a legitimate need for that information to assist with delivering a high quality, integrated safeguarding service that meets the needs of the relevant individuals. (See also Section 10 Data Sharing Governance)

Organisations signed up to this agreement commit to sharing personal data and 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 legal requirements for data protection, and which are consistent with this ISA. 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.

Area of responsibility:

Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and sharing 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 shared illegally or inappropriately.

Onward sharing of information for safeguarding purposes will be deemed appropriate where that purpose is compatible with the original purpose of sharing. Sharing of information for non-safeguarding purposes which is sourced from another organisation should be approved by the source organisation.

Each organisation should determine that 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), whether 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. Where high risk is identified and this cannot be mitigated, prior consultation with the ICO is required otherwise the processing cannot go ahead.

Persons and organisations requested to provide information for Child Death Reviews, Adult Safeguarding Reviews, Child Safeguarding Practice Reviews and Domestic Homicide Reviews must comply. Failure to comply with legislation may lead to legal action.

An individual's personal information must be accurate and up to date and will only be shared where the purpose for which it has been agreed to share clearly requires that this is necessary.

Where it is agreed that the sharing of personal information is necessary and proportionate, only that which is needed, relevant and appropriate will be shared on a 'need to know' basis.

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 organisations of personal information are kept informed of any key changes to the information that they have received, or any agreed Information Rectification requests so that records can be kept up to date.

Where information relates to a deceased individual, careful consideration must be given to the sharing of this type of information taking into account the Common Law of Confidentiality, and where applicable for Health only the Access to Health Records Act, and if necessary, further advice should be sought regarding the sharing of such data.

All organisations will ensure that Subject Access Requests and other Individual Rights requests made to them are responded to in accordance with the requirements outlined in the UK GDPR and the Data Protection Act 2018.

Area of responsibility:

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 and securely.

All staff will be made aware that sharing of personal information, where there is no lawful basis, whether inadvertently or intentionally, could be subject to disciplinary action or criminal action.

Organisations are responsible for putting into place effective procedures to address complaints relating to the sharing of personal information.

Extreme care and careful consideration should be taken where the sharing of information includes third party information and particularly personal data relating to witnesses, victims or complainants.

All organisations that process Special Category and Criminal conviction data will ensure that they have an Appropriate Policy Document (APD) in place that meets the requirements of Schedule 1, Part 4 of the data protection legislation.

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 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.

8 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 Information 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 precedence. 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 sharing can be found in Appendix 3.**

Principal law and legislation governing the protection and use of personal information is:

- a. UK General Data Protection Regulation (UK GDPR)
- b. Data Protection Act (DPA) 2018 (as amended by Data Use and Access Act 2025)
- c. Law Enforcement Directive 2018
- d. Human Rights Act 1998 (article 8)
- e. The Common Law Duty of Confidentiality

The ICO states in the [10 step guide to sharing information to safeguard children](#) 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.'* The partners to this agreement must ensure that they have the most appropriate lawful basis in place for sharing information in a safeguarding context.

As part of the provision of safeguarding services partners may encounter elements of safeguarding that have tangible links to the prevention of crime and disorder and will necessitate sharing information with 'specified authorities' (Police, Probation, Fire, Health, and Local Authorities) to prevent crime and disorder (including Anti-Social Behaviour) through the Crime and Disorder Act 1998, whereby there is a duty on these partners to:

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

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

9 Law and Guidance

The following guidance supports partners to adhere to principles defined in this agreement, the agreement is not standalone and may link to other frameworks. Please note that this list is not exhaustive.

National Guidance:

Children:

- [Working together to safeguard children](#) (Department for Education)
- [Statutory guidance: Information sharing to safeguard children and young people](#) (Department for Education)
- [10 step guide to sharing information to safeguard children](#) (Information Commissioners Office)
- [Keeping children safe in education - GOV.UK](#) (Department for Education)
- [Data sharing: a code of practice](#) (Information Commissioners Office)

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

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 2005](#) (Act of Parliament)

Preventing Crime and Disorder:

- [Information sharing for community safety - GOV.UK](#) (www.gov.uk)
- [Crime and Disorder Act 1998](#) (legislation.gov.uk)

Local Guidance:

Children:

- [South West Child Protection Procedures](#)
- [B&NES Policy and Guidance](#)
- [Keeping Bristol Safe Partnership Policy and Guidance](#)
- [South Gloucestershire Policy and Guidance](#)
- [North Somerset Policy and Guidance](#)
- [Somerset Policy and Guidance](#)

Adults:

- [B&NES Policy and Guidance](#)
- [Keeping Bristol Safe Partnership Policy and Guidance](#)
- [South Gloucestershire Policy and Guidance](#)
- [North Somerset Policy and Guidance](#)
- [Somerset Policy and Guidance](#)

Preventing Crime and Disorder:

- [B&NES Policy and Guidance](#)
- [Keeping Bristol Safe Partnership Policy and Guidance](#)
- [South Gloucestershire Policy and Guidance](#)
- [North Somerset Policy and Guidance](#)

- [Somerset Policy and Guidance](#)

10 Security Standards

Each partner is responsible for implementing appropriate physical, technical and organisational measures to ensure that data provided under this ISA is subject to sufficient security.

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.

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

- [What are 'controllers' and 'processors'? | ICO](#)
- [Contracts and liabilities between controllers and processors | ICO](#)

Where processors are used, partners should ensure that the contract/data processing agreement lists the same or higher security arrangements as the data controller.

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

It may be applicable to complete a version of the Data Security and Protection Toolkit where there are different versions depending on the size and type of organisation. The Data Security and Protection Toolkit is something which will be relevant for health care organisations and local authorities; however, the police have their own standards they adhere to. Organisations should work towards an equivalent standard depending on the type of organisation and the level of data being processed.

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.

See also Appendix 6 – Minimum Security Standards.

11 Proportionality and necessity

The data relevant under this Tier 1 Information Sharing Agreement may include personal data, special category data and criminal offence data shared for the reasons of safeguarding.

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 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 and Social Care), 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 information sharing 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.

12 Data Quality

The partners acknowledge that they have a general duty to ensure that personal data is accurate, separate to the requirement to take steps where an individual exercises the right to rectification.

The partners therefore agree:

- To have systems in place to identify any personal data that is inaccurate as to any matter of fact.
- That if partner discover that personal data is inaccurate as to any matter of fact, they will ensure that the data is made accurate and will notify any partners with whom they had shared that personal data of the accurate data.
- If they are notified that inaccurate personal data has been shared with them, they will immediately take steps to amend the inaccurate data.

- That opinions are accurate so long as they are correctly recorded. If they discover that an opinion is incorrect (for example because it is based on inaccurate data), then they will record that the opinion is incorrect.
- If they discover that they have shared an opinion which is incorrect because it is based on inaccurate personal data, they will notify any partner within whom they had shared the incorrect opinion.
- If they are notified that an incorrect opinion has been shared with them, they will immediately take steps to delete the incorrect opinion, unless it is important to retain a record of that opinion. If so, they will ensure that the record clearly shows the opinion is incorrect.

13 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 Agreement as relevant (documented justification).

Health and Social Care partners will consider the NHS England Records Management Code of Practice to inform decision making. The Constabulary (and other Police Forces) must consider and also comply with the statutory College of Policing Management of Police Information (MoPI) Code of Practice and Guidelines, also known as the Authorised Professional Practice (APP) for Police Information. Other partners will consult the relevant industry guidelines.

National inquiries must be considered when assessing records for destruction.

Information shared under this Agreement will be managed throughout its lifecycle in accordance with UK data protection legislation and each partner's retention and disposal policies. Where a sharing activity ends, or where this Agreement expires, is superseded or is terminated, partners will ensure that information is securely deleted, destroyed, anonymised, or retained under a separate lawful basis, as appropriate. No further processing of information shall take place under this Agreement once it has ended, unless such processing is supported by an alternative lawful basis and relevant governance arrangements.

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

Individuals whose personal data is processed for law enforcement purposes have the rights set out in, and subject to the provisions of, Part 3 of the Data Protection Act 2018.

14 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 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 or other agreed guidance/protocol. 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 other agreed guidance/protocol 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 sharing (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. Where automated decisions are made through the use of AI each organisation will ensure their privacy notice reflects this.

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 and organisations 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 a Partnership e.g. in respect of data reports, quality assurance or statutory reviews, then the request should be sent to the relevant Partnership Business Unit to coordinate the appropriate response. When a partner agency requires cooperation from the wider partnership to respond to an information rights request, they can contact their relevant Partnership Business Unit to ensure appropriate liaison if they have been unable to progress this within their existing processes.

15 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 the data relates are informed about the use and sharing of their information. The sharing partners will therefore agree an approach to informing individuals about the sharing of information for safeguarding purposes. This may, for example, take the form of each partner updating its own privacy information (such as a website privacy notice), or by partners referencing a shared privacy notice maintained by one or more organisations. Privacy information must be concise, transparent, intelligible, easily accessible and written in clear and plain language, tailored to children where appropriate.

Best practice in respect of transparency is to adopt a layered approach to communicating how individuals' data is used, for example through privacy notices, leaflets, letters, posters, digital communications and conversations with practitioners. However, given the nature of information sharing for safeguarding purposes, it will not always be appropriate or safe to provide full transparency. In such circumstances, partners must consider and apply the relevant exemptions under Part 2 of the Data Protection Act 2018, including where providing information would be likely to prejudice the prevention or detection of crime or cause serious harm to the physical or mental health of any individual. Where processing is carried out for a law enforcement purpose under Part 3 of the Data Protection Act 2018, the separate transparency requirements and exemptions within that regime will apply.

16 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 (security)) 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. 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 information sharing 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 sharing 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 and organisations /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. See Appendix 5 – Joint Resources.

17 Incident Management and Complaints

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 relevant data controller within 24-48 hours or as soon as reasonably possible where they become aware of an incident. Sharing partners must also determine whether other sharing partners 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 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 and/or third parties). Once a breach is recognised the relevant data controllers must be informed and will make the decision on a collaborative response to the incident. It is important to note that high risk personal data breaches must be reported to the ICO within 72 hours.

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.

18 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 Information Sharing Agreement contains high level principles and partner commitments only. It will therefore be reviewed every three years 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 the Regional Partnership Business Managers for Bristol, South Gloucestershire, North Somerset, Somerset, and Bath & North East Somerset.

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.

19 Signatories

By signing this regional T1 ISA, all signatories acknowledge and agree to comply with the obligations imposed by the ISA, as well as their respective responsibilities under data protection legislation. Signatories involved in cross-border arrangements are required to sign only one regional partnership copy of the T1 ISA, which will apply across partnerships within the Avon & Somerset region: Bristol, South Gloucestershire, North Somerset, Somerset, and Bath & North East Somerset.

Each organisation should identify who is the most appropriate post holder within their agency to sign the ISA 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 is requested to identify the post which is responsible on a day-to-day basis for monitoring compliance with this T1 ISA.

1. Signed on behalf of: Avon and Somerset Police

Name: Sarah Crew

Role: Chief Constable

Signature: Sarah Crew

Date signed: 29/09/2026

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

Regional area: Bath & North East Somerset, Bristol, North Somerset, Somerset, and South Gloucestershire

2. Signed on behalf of: Probation Service

Name: Local Probation PDU Heads

Role: Local Probation PDU Heads

Signature: Local Probation PDU Heads

Date signed: 12/08/2026

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

Regional area: Bath & North East Somerset, Bristol, North Somerset, Somerset, and South Gloucestershire

3. Signed on behalf of: Devon & Somerset Fire & Rescue Service

Name: Jon Worsley

Role: Area Manager, Devon and Somerset Fire and Rescue Service

Signature: Jon Worsley

Date signed: 12/08/2026

Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: dataprotection@dsfire.gov.uk

Regional area: Somerset

4. Signed on behalf of: Avon Fire & Rescue Service

Name: Stephen Quinton

Role: Area Manager

Signature: Stephen Quinton

Date signed: 14/07/2026

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

Regional area: Bath & North East Somerset, Bristol, North Somerset, South Gloucestershire

5. Signed on behalf of: NHS BNSSG Integrated Care Board

Name: Shane Devlin

Role: Chief Executive

Signature: Shane Devlin

Date signed: 13/08/2026

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

Regional area: Bristol, North Somerset, South Gloucestershire

6. Signed on behalf of: Somerset & B&NES NHS Integrated Care Board

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

Name: Jonathan Higman
Role: Chief Executive
Signature: Jonathan Higman
Date signed: 17/09/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: somicb.dataprotection@nhs.net / bswicb.information.governance@nhs.net
Regional area: Somerset, Bath & North East Somerset

7. Signed on behalf of: Bath & North East Somerset Council

Name: Sophie Broadfield
Role: Chief Executive
Signature: Sophie Broadfield
Date signed: 30/09/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: data_protection@bathnes.gov.uk
Regional area: Bath & North East Somerset

8. Signed on behalf of: Bristol City Council

Name: Nick Hibberd
Role: Chief Executive
Signature: Nick Hibberd
Date signed: 13/08/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: Data.protection@bristol.gov.uk
Regional area: Bristol

9. Signed on behalf of: North Somerset Council

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

Name: Mandy Bishop
Role: Chief Executive
Signature: Mandy Bishop
Date signed: 10/08/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: DPO@n-somerset.gov.uk
Regional area: North Somerset

10. Signed on behalf of: Somerset Council

Name: Duncan Sharkey
Role: Chief Executive
Signature: Duncan Sharkey
Date signed: 25/09/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: informationgovernance@somerset.gov.uk
Regional area: Somerset

11. Signed on behalf of: South Gloucestershire Council

Name: Dave Perry
Role: Chief Executive
Signature: Dave Perry
Date signed: 22/09/2026
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this ISA: DPO@southglos.gov.uk
Regional area: South Gloucestershire

Each Local Partnership Business Unit manages the complete list of signatories to this agreement for its own area.

Appendix 1 – Common sharing initiatives / area of work

This agreement covers multi-agency information sharing initiatives aimed at safeguarding children, safeguarding adults, and preventing crime and disorder across the Avon & Somerset region. It details how data is used to support these objectives. See Appendix 2 for applicable legislation / legal gateways.

Partners share information to contribute to:

Core Safeguarding, Community Safety and Crime Prevention Initiatives:

Initiative	Summary	Tier	Area
Anti-Social Behaviour Case Reviews	Multi-agency review of repeat/serious ASB cases to assess risk and coordinate intervention when complainant is not satisfied with agencies/organisations responses	T2	B&NES Bristol North Somerset Somerset South Gloucestershire
Child Death Overview Panel (CDOP)	Review of child deaths to identify learning and prevent future deaths.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Child Death Reviews	Statutory review process to understand causes and learning when a child dies.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Child Safeguarding Practice Reviews (CSPR)	Reviews of serious child safeguarding incidents identifying learning. Includes Rapid Review process.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Serious Incident Notifications	Information checks and exchanges to inform urgent child protection decisions.	T1	B&NES Bristol North Somerset

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

			Somerset South Gloucestershire
DASH (Domestic Abuse, Stalking, Harassment, Honour-based Violence)	Sharing on victims/perpetrators to assess risk and manage safety.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Domestic Homicide Reviews (DHR) / Domestic Abuse Related Death Reviews (DARDRs)	Statutory review of domestic abuse-related deaths.	T1	B&NES North Somerset Somerset South Gloucestershire
LADO (Local Authority Designated Officer) Allegations Management / PiPoT (Person in a Position of Trust)	Managing allegations against professionals and persons in a position of trust through information exchange.	T1	B&NES North Somerset Somerset South Gloucestershire
Modern Slavery	Multi-agency sharing on victims/perpetrators; NRM and DtN referrals.	T1	B&NES North Somerset Somerset South Gloucestershire
MARAC - Multi-Agency Risk Assessment Conference	Multi-agency meeting for high-risk domestic abuse victims.	T2	B&NES North Somerset Somerset South Gloucestershire
MASH - Multi-Agency Safeguarding Hub	Multi-agency triage using rapid, proportionate information exchange.	T2	B&NES North Somerset Somerset South Gloucestershire
MAPPA - Multi-Agency Public Protection Arrangements	Multi-agency management of serious violent/sexual offenders.	T2	B&NES North Somerset Somerset South Gloucestershire
Operation Encompass	Police share Domestic Abuse notifications with schools to safeguard children - subject to local authority providing education data. Information sharing duty: Operation Encompass	T2	B&NES North Somerset Somerset South Gloucestershire

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

Prevent & Channel	Early intervention for individuals at risk of radicalisation.	T1	B&NES North Somerset Somerset South Gloucestershire
Serious Violence & Exploitation	Actions to reduce serious violence/exploitation – including Violence Reduction Partnerships	T2	B&NES North Somerset Somerset South Gloucestershire
Quality Assurance, Inspection & Scrutiny	Data used to evaluate system performance.	T1	B&NES North Somerset Somerset South Gloucestershire
Safeguarding Adult Reviews (SAR)	Learning from serious adult safeguarding incidents.	T1	B&NES North Somerset Somerset South Gloucestershire
Section 47 (Children Act)	Multi-agency enquiries into significant harm.	T1	B&NES North Somerset Somerset South Gloucestershire
Section 20 (Children Act)	Sharing information about children accommodated voluntarily.	T1	B&NES North Somerset Somerset South Gloucestershire
Section 17 (Children Act)	Multi-agency sharing supporting children in need.	T1	B&NES North Somerset Somerset South Gloucestershire

Additional Statutory Child Safeguarding Processes:

Initiative	Summary	Tier	Area
Strategy Discussions	Initial multi-agency information exchange to determine S47 threshold.	T1	B&NES North Somerset Somerset South Gloucestershire

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

Initial Child Protection Conference	Multi-agency meeting to assess risk and determine CP Plan.	T1	B&NES North Somerset Somerset South Gloucestershire
Review Child Protection Conference	Review of CP Plan progress and agency activity.	T1	B&NES North Somerset Somerset South Gloucestershire
Child Protection Plans	Ongoing multi-agency oversight of actions and interventions.	T1	B&NES North Somerset Somerset South Gloucestershire
Pre-Proceedings (PLO - Public Law Outline)	Multi-agency information to support decisions ahead of care proceedings.	T1	B&NES North Somerset Somerset South Gloucestershire
Early Help Panels	Joint discussions to support families early.	T2	B&NES North Somerset South Gloucestershire
Contextual/Risk Outside the Home Safeguarding Panels	Sharing on risks outside the home (peer groups, locations).	T2	Somerset South Gloucestershire
Youth Justice / Youth Offending Team / Youth Justice Service	Multi-agency planning for children in the youth justice system.	T2	B&NES North Somerset Somerset South Gloucestershire
CIC (Child in Care) Planning & Reviews	Multi-agency sharing for care planning, placement and return home.	T1	B&NES North Somerset Somerset South Gloucestershire
Families First Partnership	Local Family Help, family group decision-making and Multi-Agency Child Protection Teams (MACPTs).	T2	B&NES Bristol North Somerset Somerset South Gloucestershire

Additional Statutory Adult Safeguarding Processes:

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

Initiative	Summary	Tier	Area
Section 42 Enquiries	Multi-agency action to assess and manage adult safeguarding concerns.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Self-Neglect Panels	Cross-agency review for adults at high risk.	T2	
MARM - Multi-agency Risk Management	Multi-agency process to jointly manage risks for adults with complex needs outside Section 42 safeguarding.	T2	B&NES Bristol North Somerset Somerset South Gloucestershire
Hoarding Panels	Multi-agency risk management for hoarding behaviour.	T2	
LPS - Liberty Protection Safeguards / DoLS - Deprivation of Liberty Safeguards	Information sharing for assessments and authorisations safeguarding adults lacking capacity.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire

Additional Community Safety Partnership Processes:

Initiative	Summary	Tier	Area
Disruption Panel	Multi-agency management of serious organised crime.	T2	South Gloucestershire North Somerset Somerset
High-Risk Perpetrator Panels (DRIVE)	Multi-agency risk management of serial DA perpetrators.	T2	Bristol North Somerset South Gloucestershire
VAWG Panels	Coordination on violence against women and girls.	T2	
Hate Crime Panels	Multi-agency risk management for hate crime victims/perpetrators.	T2	
Integrated Offender Management (IOM)	Multi-agency offender management.	T2	
Local Criminal Justice Board	Strategic information sharing across justice services.	T1	B&NES Bristol North Somerset

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

			Somerset South Gloucestershire
Anti-Slavery Partnerships	Multi-agency sharing on trafficking/exploitation.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Reducing Reoffending Board	Strategic information sharing.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Contest Board	Counter Terrorism.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire

Cross-Cutting Multi-Agency Processes:

Initiative	Summary	Tier	Area
Escalation / Professional Disagreement	Case-specific sharing to resolve disagreements.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Independent Scrutiny & Annual Reporting	Data shared for partnership oversight.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire
Multi-Agency Audits & Learning	Data used in audits and thematic learning.	T1	B&NES Bristol North Somerset Somerset South Gloucestershire

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 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.

Appendix 2 - Applicable Legislation

It is not exhaustive, and each organisation must be satisfied that they have checked and verified their own legal gateways for processing the information being shared. However, it provides a comprehensive statutory foundation for information sharing under this Tier 1 Agreement, and a quick-reference tool to:

- guide to lawful gateways
- support DPIAs and Tier 2 ISAs
- strengthen decision-making during multi-agency meetings
- provide assurance to audit, scrutiny and oversight bodies

Children's Safeguarding Legislation & Gateways:

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
1	Children Act 1989	s.17, s.20, s.27, s.47	Child in Need, accommodation, duty to cooperate, significant harm enquiries	LA, Police, Health, ICB	Children
2	Children Act 2004	s.10, s.11, s.16E, s.16LA	Multi-agency cooperation; safeguarding duties, Information Sharing Duty	LA, Police, ICB, Schools	Children

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
3	Working Together to Safeguard Children	Statutory guidance	Strategy discussions, CP conferences, early help, contextual safeguarding	All safeguarding partners	Children
4	Children and Families Act 2014	ss.23–25	SEN duties; integrated education, health & care planning	Health, LA	Children
5	Children (Leaving Care) Act 2000	Amendments to CA1989	Supporting care leavers with education, training, wellbeing	LA	Children
6	Childcare Act 2006	s.1, s.3	Duties to improve wellbeing and integrate early years services	LA, Police	Children
7	Education Act 2002	s.175, s.157	Safeguarding duties for schools and FE settings	LA, Schools	Children
8	Education Act 1996	Identifying children missing education	CME safeguarding and welfare	Schools, LA	Children
9	Education (Independent Schools Standards) Regs 2003	Schedule, Section 3	Safeguarding duties in independent schools	Independent schools	Children
10	Mental Capacity Act 2005	Various	Decision-making for 16–17-year-olds lacking capacity	LA, NHS, Police, YOT	Children 16+
11	Domestic Abuse Statutory Guidance 2022	ss.248, 439, 443, 445	Operation Encompass; safeguarding children affected by DA	Police, LA, Schools	Children
12	Victims and Prisoners Act 2024	Operation Encompass duty	Police notifications of DA incidents to schools	Police, Schools	Children

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
13	Children's Wellbeing and Schools Act 2026	Various	Multi-agency cooperation; safeguarding duties, Duty to Share, Family Help, MACPT, Consistent Identifier	All safeguarding partners	Children

Adult Safeguarding Legislation & Gateways:

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
1	Care Act 2014	ss.1–3, 6–7, s.42, s.45	Wellbeing, prevention, cooperation, S42 enquiries, SAB information duty	LA, Health, Police	Adults
2	Mental Capacity Act 2005	Various	Best-interest decisions, DoLS, LPS, safeguarding adults lacking capacity	LA, NHS, Police	Adults
3	Health & Social Care Act 2012	s.195	Integration duties, sharing for wellbeing	NHS, LA	Adults
4	Health & Social Care (Quality & Safety) Act 2015	s.3, s.251B	Sharing across health and social care providers	Health, LA	Adults
5	NHS Act 1977 & NHS Act 2006	s.22 (1977), s.82 (2006)	Duty to cooperate for health/welfare	NHS, LA	Adults
6	NHS & Community Care Act 1990	—	Notifying partner agencies/organisations during assessments	NHS, LA	Adults
7	Domestic Abuse Statutory Guidance 2022	Relevant sections	Adult victim safeguarding, MARAC, high-risk DA cases	Police, LA, NHS	Adults

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
8	Modern Slavery Act 2015	Various	NRM referrals; adult exploitation cases	All First Responders	Adults
9	Immigration & Asylum Act 1999	s.20	Sharing for immigration control, asylum support	Public Authorities	Adults
10	Welfare Reform Act 2012	s.131	Welfare-related data sharing	LA, DWP	Adults
11	Social Security (Information Sharing) Regs 2012	s.131(3)	Supporting Families / welfare data exchange	LA & Schools	Adults

Community Safety Partnership (CSP) & Crime Prevention Gateways:

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
1	Crime and Disorder Act 1998	s.17, s.37, s.115	Preventing crime/ASB; Youth Justice; information sharing powers	Police, LA, Health	Both
2	Criminal Justice Act 2003	s.325–327 (MAPPA)	Multi-agency public protection	Police, Probation, LA, Health	Both
3	Serious Violence Duty (PCSCA 2022)	—	Multi-agency data sharing to prevent serious violence	Police, LA, Health, Probation, Fire & Rescue	Both
4	Domestic Violence, Crime and Victims Act 2004	s.9 DHRs	Domestic Homicide Reviews	Police, LA, Probation	Both
5	Counter-Terrorism and Security Act 2015	s.29, s.38	Prevent Duty and Channel cooperation	Police, LA, NHS, Education	Both
6	Counter-Terrorism & Border Security Act 2019	—	Reinforces Prevent information sharing duties	Police, LA, Schools	Both

Overarching Tier 1 Safeguarding Children and Adults and Preventing Crime and Disorder Information Sharing Agreement

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
7	Modern Slavery Act 2015	—	Human trafficking; exploitation	All First Responders	Both

Cross-Cutting Multi-Agency and Public Protection Gateways:

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
1	Data Protection Act 2018	Part 2, Part 3, Sch.1	Processing of general, special category & criminal offence data	All	Both
2	UK GDPR	Art.6, Art.9, Art.10	Lawful bases for processing; safeguarding; public task	All	Both
3	Common Law Duty of Confidentiality	—	Sharing when justified by law, public interest or consent	All	Both
4	Human Rights Act 1998	Article 8	Proportionate interference to protect life & prevent harm	All	Both
5	Local Government Act 2000	s.2	Wellbeing powers enabling lawful cooperation	LA	Both
6	Localism Act 2011	General Power of Competence	Cooperation unless prohibited by other laws	LA	Both
7	Health & Social Care (Quality & Safety) Act 2015	s.3, s.251B	Sharing across H&SC sectors	NHS, LA	Both

	Legislation	Relevant Sections / Powers	Typical Use Cases	Partners	Adults / Children
8	Supporting Families Programme Gateways	Welfare Reform Act 2012 ; Social Security (Information Sharing) Regs 2012	Targeted family support; multi-agency data sharing	LA, Schools, DWP	Both

Appendix 3 – Joint Resources

Contact the relevant partnership for more information on local 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 4 - Information sharing principles

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 and organisations. 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 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 5 - Collaborative Data Breach Process

Organisations must ensure that they are able to recognise and report potential personal data breaches immediately. Staff should escalate incidents to their organisation's data protection lead (e.g. DPO or IG team) without delay. In a multi-agency context, where shared data is involved, organisations must also notify counterpart organisations right away so a coordinated response can begin.

Contain the breach - Organisations must act swiftly to prevent further data loss (e.g. stop the data flow, secure compromised accounts, and retrieve missent documents). Organisations must assess the scope and risks, and determine what personal data is affected, how many individuals, and the potential impact (e.g. risk of harm, distress, or fraud). Upon becoming aware of a breach, it should be addressed promptly, isolating issues and evaluating adverse consequences for individuals to inform next steps such as notifications.

Multi-Agency Communication & Lead Coordination - Organisations must inform all partner organisations whose data is impacted as soon as a breach is suspected. Designate a lead organisation to coordinate the joint response (this is often the organisation where the breach occurred or the data controller for the shared data). The lead organisations incident manager or DPO will oversee the action plan, decision-making, and communication. All organisations should stay in close contact (e.g. via an incident conference call or joint task force) to share updates and ensure everyone is fulfilling their roles.

Each organisation will determine whether to self-report, or whether the lead organisation (on behalf of all involved controllers) will report it to the Information Commissioner within 72 hours of becoming aware of a reportable breach.

If the breach is likely to result in a high risk to individuals' rights and freedoms, you must inform the affected individuals as soon as possible and without undue delay. Organisations should coordinate with each other to decide who will contact the individuals, for example the organisation with the direct relationship should usually lead, with input from others.

Investigation & Record-Keeping - Investigate the incident thoroughly to determine how and why it occurred. The organisations should work together to trace the timeline, identify the root cause (e.g. human error, system failure, security gap), and catalogue all affected data. Each organisation must document the breach and its response including facts about what happened, the effects, and remedial actions taken in their breach log or register. The lead organisation should compile a summary report and circulate it to partners.

Remediation & Lessons Learned - Mitigate any ongoing risks and address weaknesses revealed by the breach. This could involve revoking or changing credentials, patching software, improving encryption, or tightening access controls. If human error or process failure was a factor, implement improvements: e.g. strengthen verification steps, update policies/procedures, or provide refresher training to staff.

Multi-agency teams should jointly review the incident and learn lessons to evaluate what worked and what didn't in the response. Once all actions are completed, ensure each organisation's leadership is briefed and that the incident is formally closed in your records with a view toward continuous improvement.

Appendix 6 – Minimum Security Standards

The partners agree to protect the physical security of the shared data.

This means they will, as a minimum:

- Ensure their organisation controls physical access to its premises;
- Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises;
- Ensure proper physical control of printers and photocopiers so that personal data is not left lying on printers/photocopiers;
- Ensure secure disposal of printed materials, so that materials intended for disposal do not remain accessible. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises;
- Ensure that old computers, printers and other electronic equipment are disposed of safely and that all personal data is irretrievably deleted from any memory before disposal.

The partners agree to protect the electronic security of the shared data. This means they will, as a minimum:

- Ensure their organisation has a strong password policy that is adhered to by all personnel. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members;
- Ensure their organisation installs security patches on electronic devices (including ensuring all operating systems' updates are installed in line with best practice);
- Ensure personnel are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work;
- Ensure that any Wi-Fi connections are secure and that any guest Wi-Fi is on a segregated system, so that guests cannot access other systems from that Wi-Fi;
- Ensure that any data that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice;
- Ensure that their organisation complies with the best practice of cyber security as detailed by the National Cyber Security Centre.

The partners agree to ensure that all shared data held on portable devices, including laptops, tablets and USB/portable drives, has full disk encryption. This must be to industry standard, and as a minimum:

- FIPS 140-2/256 bit asymmetrical encryption; or

- CBC-AES 256-bit encryption. A recognised mark of excellence in encryption is CCTM government accreditation (for more information, see the National Cyber Security Centre website).

The partners shall e-mail special category personal data or information about individuals' criminal convictions or offences, suspected or otherwise, only via secure e-mail.

Appendix 7 - 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)

Overarching Tier 1 Child Safeguarding, Adult Safeguarding and Community Safety Information Sharing Agreement

Term	Definition
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.
Consistent Identifier	Children's Wellbeing and Schools Act introduces a clear legal duty to share information for the purposes of safeguarding and promoting the welfare of children, including the forthcoming implementation of a Consistent Identifier, to be specified and the organisations required to use it via regulations. Also referred to as Single Unique Identifier.
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.
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.
Information Sharing Agreement (ISA)	Terminology can vary (Information Sharing Agreement, Data Sharing Agreement, 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.

Overarching Tier 1 Child Safeguarding, Adult Safeguarding and Community Safety Information Sharing Agreement

Term	Definition
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 December 2031).
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 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.
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.

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 ISA	In this document Tier 1 Information Sharing Agreement can be understood as an overarching Multi Agency Safeguarding Information 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 ISA, Information Sharing Protocol, Data Sharing Charter, and others.
Tier 2 ISA	In this document a Tier 2 Information 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. It should be read alongside the DPA 2018.
Data Use and Access Act	Legislation that changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.

Appendix 8 – Information Governance Contact

Organisation	Address	ICO registration number	Compliance contact person	Contact details
Avon & Somerset Constabulary	Valley Road, Portishead, Bristol BS20 8JJ	Z4882079	Data Protection Officer	dpo@avonandsomerset.police.uk

Overarching Tier 1 Child Safeguarding, Adult Safeguarding and Community Safety Information Sharing Agreement

Bath & North East Somerset Council	Bath & North East Somerset Council Guildhall, High Street, Bath BA1 5AW	Z5664161	Data Protection Officer	data_protection@bathnes.gov.uk
North Somerset Council	Walliscote Grove Road, Weston-super-Mare, BS23 1UJ	Z6519259	Data Protection Officer	DPO@n-somerset.gov.uk
Bristol City Council	City Hall, College Green, Bristol, BS1 5TR	Z5873747	Data Protection Officer	Data.protection@bristol.gov.uk
Somerset Council	County Hall, Taunton TA1 4DY	Z5957592	Data Protection Officer	informationgovernance@somerset.gov.uk
South Gloucestershire Council	Badminton Road, Yate, Bristol, BS37 5AF	Z5077191	Data Protection Officer	DPO@southglos.gov.uk CAHDataProtection@southglos.gov.uk
NHS BNSSG Integrated Care Board	100 Temple Street, Redcliffe, Bristol, BS1 6AG	Zb344972	Caldicott Guardian	Bnssg.foi@nhs.net
Somerset & B&NES (cluster) NHS Integrated Care Board NHS Somerset Integrated Care Board & Bath and North East Somerset, Swindon & Wiltshire	Somerset ICB Wynford House Lufton Way Lufton Yeovil BA22 8HR	ZB363198	Data Protection Officer	somicb.dataprotection@nhs.net
	BSWICB Jenner House Avon Way Langley Park Chippenham SN15 1GG	ZB524371	Data Protection Officer	bswicb.information.governance@nhs.net

Overarching Tier 1 Child Safeguarding, Adult Safeguarding and Community Safety Information Sharing Agreement

Integrated Care Board				
Probation Service	102 Petty France, London, SW1H 9AJ	Z5679958	Data Protection Officer	dpo@justice.gov.uk
Devon & Somerset Fire & Rescue Service	The Knowle Clyst St George, Exeter, Devon EX3 0NW	Z5462624	Data Protection Officer	dataprotection@dsfire.gov.uk
Avon Fire & Rescue Service	Police & Fire Headquarters PO Box 37 Valley Road Portishead Bristol BS20 8JJ	Z6748396	Data Protection Officer	DPO@avonfire.gov.uk FOI-DP@avonfire.gov.uk

Each Local Partnership Business Unit manages the complete list of signatories to this agreement for its own area.