

## INFORMATION SHARING:

### SECOND LEVEL PROTOCOL FOR DATA SHARING FOR

### BRISTOL NORTH SOMERSET AND SOUTH GLOUCESTERSHIRE INTEGRATED CARE BOARD (BNSSG ICB) SAFEGUARDING

#### 1. Purposes & Benefits of Information Sharing

Safeguarding means protecting a citizen's health, wellbeing and human rights; enabling them to live free from harm, abuse and neglect. Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding adults, unborn baby, children, and young people.

The “**Purpose**” of this Information Sharing Agreement is to provide a framework to facilitate the appropriate sharing of information for Safeguarding purposes by Bristol, North Somerset, and South Gloucestershire Integrated Care Board (BNSSG ICB) and within the Integrated Care System (ICS) with the three Local Authority Safeguarding Adult Boards (SABs), Children Safeguarding Partnerships (CSPs), Community Safety Partnerships, Police Constabulary and their other partner agencies.

#### 2. Role & Responsibilities of Partners

Each organisation is the controller of and responsible for the information they receive under this agreement. BNSSG Safeguarding is a multi-agency partnership between:

- BNSSG Integrated Care Board
- BNSSG General Practices
- Avon and Wiltshire Partnership (AWP) Mental Health Trust
- University Hospitals Bristol and Weston NHS Foundation Trust (UHBW)
- North Bristol NHS Trust (NBT)
- Sirona Care and Health
- South Western Ambulance Service NHS Foundation Trust
- Bristol City Council.
- North Somerset Council
- South Gloucestershire Council
- Avon and Somerset Constabulary

Other strategic partnerships and organisations that have responsibilities to address issues relevant to safeguarding children and adults

## **2.1: Information Sharing and Safeguarding Activity**

Health partners share information to contribute to:

- Rapid Reviews
- Safeguarding Adult Reviews (SARS)
- Domestic Homicide Reviews (DHRs)
- Child Safeguarding Practice Reviews (CSPRs)
- Serious Case Reviews
- Channel Panel Meetings (PREVENT agenda)
- Female Genital Mutilation reporting
- MARAC (Multiagency Risk Assessment Conference)
- MAPPA (Multiagency Public Protection Agency)
- MASH (Multiagency Safeguarding Hub)
- MARM (Multiagency Risk Management)
- Modern Slavery (National Referral Mechanism)
- NHSE platform and data collation
- PREVENT
- Safeguarding Quality Assurance Audits
- Section 42 Enquiries
- Section 47 Enquiries
- Individual Safeguarding
- Organisational Safeguarding
- Patient Safety Incident Response Framework (PSIRF)
- Serious Violence Duty

## **3. Relevant Legislation, Standards and Guidance**

The Information Sharing Agreement is underpinned by the following legislation, statutory and policy guidance and will be applied as necessary (the following list is not exhaustive)

- Human Rights Act 1998
- Data Protection Act 2018
- UK-General Data Protection Regulations (UK-GDPR)
- Caldicott Principles
- The Children and Social Work Act 2017 (under which the named BNSSG local authority area, Chief Officer of Police for the named area, and BNSSG ICB have an equal and shared duty to work together (in partnership with other relevant agencies) to decide to safeguard and promote the welfare of all children on BNSSG ICS.
- Children's Act 1989 S47
- The Children Act 2004, sections 10, 11 and 16A – 16L
- The Care Act 2014 (including statutory guidance to the Care Act 2014) which requires the establishment of a Safeguarding Adults Board (SAB) comprising the local authority, BNSSG ICB, the BNSSG local authority's area and the Chief Officer of Police, to assure itself that local safeguarding arrangements and partners act to help and protect adults.
- Crime and Disorder Act 1998, section 115
- The Criminal Justice Act 2003, section 325
- Serious Violence Duty 2022
- Domestic Violence Act 2021

- Working Together to Safeguard Children statutory guidance July 2018
- Information Sharing Advice to practitioners providing safeguarding services to children, young people, parents, and carers July 2018.

#### 4. Lawful Basis for Sharing, Approach to Consent, Legal Duty or Legal Powers to Share

Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, The UK-GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data.

- The UK-GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children, young people and adults safe.
- To effectively share information: all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role.
- Information which is relevant to safeguarding will often be data which is considered ‘special category personal data’ meaning it is sensitive and personal where practitioners need to share special category personal data. All practitioners should be aware that the Data Protection Act 2018 includes ‘safeguarding of children and individuals at risk’ as a condition that allows practitioners to share information without consent.
- The UK-GDPR sets out that, in order to be able to process personal and special category personal, data about an individual it is necessary to identify an appropriate lawful basis of processing. These are set out in detail in Articles 6 and 9 of the UK-GDPR. For safeguarding purposes, the principal lawful basis of processing are:
  - Consent: but it is vital to understand that information can be lawfully shared without consent, if a practitioner is unable to or cannot be reasonably expected to gain consent from the individual concerned (such as when an individual lacks the necessary mental capacity<sup>1</sup>), or if to gain consent could place a child or adult at risk. Consent is also not required where sharing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
  - Public task: information sharing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  - Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional, or mental harm, or if it is protecting their physical, mental, or emotional well-being.
  - Information sharing where it is necessary for the establishment, exercise or defence of legal claims.
  - Information sharing where it is necessary for reasons of substantial public interest.
- The information of a deceased individual is not dealt with under the UK-GDPR / DPA 2018. When sharing information of a deceased individual the common law duty of confidentiality will be considered to ensure that the share is fair and legal.
- **The following tables details the various purposes for which safeguarding information may be shared along with the legislation or standards that support the sharing of information.**

Framework/Process	Reference
Rapid Reviews	Working Together to Safeguard Children (2018) Children Act 1989 Children Act 2004 Children and Social Work Act 2017

<sup>1</sup> Sections 1 – 3 Mental Capacity Act 2005

Child Safeguarding Practice Reviews	Working Together to Safeguard Children (2018) Children Act 2004
Safeguarding Adult Reviews (SARs)	Care Act 2014
Domestic Homicide Reviews (DHRs)	Domestic Violence Crime and Victims Act 2004
Channel Panel Meetings (PREVENT agenda)	Counter Terrorism and Security Act 2015 Crime and Disorder Act 1998
Female Genital Mutilation reporting	Female Genital Mutilation 2003 Health and Social Care Act 2012
MARAC (Multi Agency Risk Assessment Conference)	Crime and Disorder Act 1998
MAPPA (Multi Agency Public Protection Agency)	Criminal Justice Act 2003
MASH (Multi Agency Safeguarding Hub)	Working Together to Safeguard Children (2018) Children Act 1989 Children Act 2004 Children and Social Work Act 2017
MARM (Multi Agency Risk Management)	Care Act 2014 Crime and Disorder Act 1998
Modern Slavery (National Referral Mechanism)	Modern Slavery Act 2015 Crime and Disorder Act 1998
NHSE Case Review Tracker Platform	Health and Social Care Act 2012
PREVENT	Counter Terrorism and Security Act 2015
Safeguarding Quality Assurance Audits	Working Together to Safeguard Children (2018) Care Act 2014
Section 42 Enquiries	Care Act 2014
Section 47 Enquiries	Children Act 1989
Individual Safeguarding	Care Act 2014
Organisational Safeguarding	Care Act 2014
Patient Safety Incident Response Framework (PSIRF)	NHS Patient Safety Strategy
Serious Youth Violence	Serious Violence Act 2022 Domestic Abuse 2021

## 5. Information Exchanged or Shared Between Partners

All signatories are committed to ensuring the accuracy and completeness of data exchanged, should any inaccuracies be identified recipient organisations will be informed so that appropriate steps can be taken including a process for informing all relevant parties of any inaccuracies identified.

Information shared is patient health, social care and/or police records held electronically or on paper documents. Patient health records are those completed and stored on Connecting Care system or in individual health organisation electronic or paper systems.

Social care and police records are those relating to people contact with services and are held on electronic record systems.

Who are the Data Subjects?	BNSSG population
----------------------------	------------------

What Level of identity will be shared?	Data will be anonymised when appropriate, however identifiable information will be shared under this agreement.
What fields of data will be shared?	Relevant and necessary information will be shared, this may contain any information held on individuals record
What is the source of the data?	Patient Health/social care or police record
Will multiple datasets be linked?	No
How long will data be retained by the recipient organisation	For duration of the safeguarding statutory review being undertaken

## 6. Security

All parties shall ensure compliance with the Data Protection Act 2018, UK-GDPR and all other applicable legislation including the Human Rights Act 1998.

All parties accept that the information shared is confidential and will only process the information for the purposes outlined in this agreement or where the processing is required/permitted by law.

Transfer of information by secure encrypted methods. Appropriate technical and organisational security measures will be taken to protect all shared information from unauthorised use, access, loss, destruction, theft or disclosure of the information.

All parties shall ensure they keep the Shared Personal Data for no longer than is necessary for the Purpose or that Partner Agency's statutory functions.

## 7. Individual's Rights

See section 4 for detail. Individuals, relatives and carers will be informed of the sharing of information when required and permitted under law. Duty of candour<sup>2</sup> will be followed in the completion of BNSSG safeguarding statutory reviews and completed published reports. BNSSG ICB will undertake duty of candour and complaint and grievance processes as required for any individual, relative or carer as required.

## 8. Incident Management

Should a party become aware of any unauthorised access or unlawful processing or Information Governance issue they will notify the other relevant parties as a matter of priority and in any event within 48 hours of discovery to allow notification to be made to the ICO within the 72-hour time limit if necessary. All breaches of security must be dealt with in accordance with organisational policies and practices and externally reported as required. Where required the Information Governance Leads from relevant organisations will investigate jointly.

## 9. Complaints Procedures

Signatories will use their own organisational procedures to deal with complaints which arise from information sharing under this Agreement.

## 10. Awareness Training/Communication to Involved Individuals

All staff will be appropriately trained in Data Protection and Confidentiality and access to personal data will be limited to staff who require access for the performance of their duties.

<sup>2</sup> [Duty of candour - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

## **11. Monitoring & Review**

This agreement will be reviewed on an annual basis and compliance with the requirements will be monitored by Rosi Shepherd Chief Nurse.

Signed for and on behalf of: **Organisation Name**

Name:

Job Title:

Signature:

Date:

Signed for and on behalf of: **Organisation Name**

Name:

Job Title:

Signature:

## Appendix One

### **Lawful bases for processing?**

The lawful bases for processing personal data are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The lawful bases for processing special categories of personal data are set out in Article 9 of the UK GDPR. At least one of these must apply whenever you process special category data:

(a) Explicit consent

(b) Employment, social security and social protection (if authorised by law)

(c) Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving, research and statistics (with a basis in law)