Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Multi-Agency Overarching Information Sharing Agreement Tier 1

A standard overarching information sharing Agreement which can be used by all agencies within Avon and Somerset Constabulary policing area for sharing personal data

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy.
Amendments may occur at any time and you should always consult the principle electronic file or contact the Protocol owner for the latest version.

Contents

Version Control			
Edit	**Author**	**Version**	**Date**
Draft version raised at Chief Executives meeting (A&S Police HQ) for consultation	Jeff Hines	0.1	10.12.12
Final draft version	Jeff Hines	1.0	09.05.13
Minor revisions.	Jeff Hines	1.1	17.06.13
Agreement authorised by Acting Assistant Chief Constable Hayler, Avon an d Somerset Constabulary	Jeff Hines	1.2	17.06.13
Agreement reviewed. Meeting held at Police HQ with interested parties. Indemnity removed and minor format changes made.	Jeff Hines	1.3	26.06.14
Revised Agreement published	Jeff Hines	2.0	02.09.14
Bristol City Council Log added	Jeff Hines	2.1	19.09.14
South Gloc Council logo added	Jeff Hines	2.2	15.08.15
Original Protective Markings removed – document is OFFICIAL.- no markings required Document Reviewed Appendix B examples of signatory and date changed to Andy Marsh and March 2017	Jeff Hines	2.3	21.03.17
Revisions to reflect the changes to data protection legislation – GDPR and Data Protection Act 2018	Ellena Talbot	3	12.07.18
Minor changes of the author/owner of the document and reviewing schedule,	Kate Britton	3.1	05.02.19
Change GDPR > UK GDPR, email address	Kate Britton	3.2	24.06.21

Section 1 Protocol Information

Protocol Information	Reviewed by: (Name, Area/Dept.)	Date:
Signed off by Head of Department/Area:	Kate Britton, Data Protection Officer	February 2019
Reviewed for Code of Ethics Compliance:	Kate Britton, Data Protection Officer	February 2019
Start date:	June 2013	
Last reviewed:	June 2021	
Next due for review:	June 2023	

Section 2 About this Document

2.1 This Protocol is hosted by Avon and Somerset Constabulary, and came in to effect on 17th June 2013, and has subsequently been reviewed and amended in accordance with UK GDPR/The Data Protection Act 2018.

2.2 It provides a standard overarching Protocol which can be used by all agencies within the Avon and Somerset Constabulary policing area for sharing personal data.

2.3 This Protocol (Tier 1) sets the guiding principles, ethos and standards for data sharing common to all agencies and is signed off once by the respective chief executive or equivalent.

2.4 An ISA Tier 2 can be used for all data sharing, ad hoc or regular, and it should be signed off by local managers; asset owners; asset assistant; asset guardians or custodians, anybody who consider themselves accountable for the data and the data exchange.

2.5 Over time this Protocol will supersede all existing agreements between Avon and Somerset Constabulary and other agencies.

2.6 Contact or queries in relation to this agreement should be directed to:

The Data Protection Officer
Legal Services
Avon and Somerset Constabulary Police HQ
Valley Road
PO Box 37
Portishead
Bristol
BS20 8QJ
E-mail: *InformationSharing@avonandsomerset.police.uk*

Section 3 Policy Statement and Purpose of this Document

3.1 The significant benefits to service users, the wider public and to the legitimate activities of our organisations, derived from sharing timely, relevant and accurate data, both personal and other, have now long since been established. The widely recognised value and success of data sharing has however generated a plethora of agreements or protocols as they are sometimes known, being developed between various partner agencies.

3.2 Although it is not always a legal requirement, it is good practice to have an Information Sharing Agreements (ISA) in place where there is regular or semi-regular sharing of data, particularly personal data. Where disclosures are 'one off' in nature or do not involve personal data, there is no requirement for an ISA. For the purposes of this document the terms Information Sharing Protocol and Information Sharing Agreement are interchangeable and have the same meaning.

3.3 Whilst this document prescribes the minimum acceptable standards at key stages of the sharing process, it will always be the responsibility of each partner to ensure that they comply with any legislation, national standards and local policy(s) applicable to them or to the processes in which they are engaged.

3.4 By setting the minimum standards and expectations for multi-agency data sharing, the intention of this document is to replace the need for lengthy future agreements by underpinning them with these guiding principles. It is envisaged that in future all ISAs, current and new, will be short, specific and user friendly

3.5 One of the guiding principles of this Protocol is that there is a clear expectation that parties to this agreement share data in accordance with the requirements of the Data Protection Act 2018, the General Data Protection Regulation and any applicable Data sharing Code of Practice (Information Commissioners Office- www.ico.gov.uk). There is also an expectation that the terms of the Human Rights Act 1998 and other relevant legislation.

3.6 This Protocol (Tier1) provides an overarching agreement which sets out the guiding principles and ethos of data sharing between the signatories to this Protocol. This is signed off once by or on behalf of a chief officer or equivalent for each organisation.

3.7 The second tier is the specific agreement between the signatories for the sharing of personal data. Tier 2 ISAs can be signed off locally by a senior manager or practitioner who has the authority to act on behalf of their organisation. A template that should be used for all future Tier 2 ISAs can be found at Appendix A to this Protocol

3.8 It is important to note that this is an overarching Protocol to formalise the regular sharing of information. It does not interfere with or otherwise prevent the sharing of information on an adhoc basis in accordance the provision(s) under Article 6 of the UK GDPR and where relevant Section 8 of the Data Protection Act 2018, to the extent that such processing is necessary in the public interest

Section 4 What do we mean by 'Data Sharing?'

4.1 For the purpose of this Protocol the terms "data sharing" and "disclosure" have the same meaning and refer to the release of data from one organisation to one or more other organisations.

Section 5 Personal Data

5.1 This Agreement deals solely with personal data[1]. Personal data should only be shared where it is necessary and lawful to do so. At all times those sharing personal data should remember the need to ensure that such data is processed lawfully and fairly in relation to the data subject. Where personal data is to be disclosed the following sections will apply.

Section 6 Legal Basis

6.1 In order to share personal data, there needs to be a relevant legal gateway. It is important to note that the existence of an ISA or Protocol does not provide a legal gateway or secure an automatic right to share information with or from another organisation.

6.2 Each signatory must be able to identify their lawful basis to share personal data. This may come from statute, common law or legal precedence. For the purposes of this Protocol sharing will be reliant upon a statutory or common law power. Statutory powers will differ between the signatory organisations and cannot be prescribed in this Protocol, but in broad terms a statutory power can be an express obligation or an express power and are often referred to as legal gateways.

6.3 Express Obligations: (a duty) - occasionally, a public body will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances but, where such an obligation applies, it is clearly permissible to share the information.

[1] As defined by Article 4 UK GDPR and Part 1, Paragraph 3 of The Data Protection Act 2018

6.4 Express Powers: (a power) - sometimes, a public body will have an express power to share information, but it does not compel them to do so. An express power will often be designed to permit disclosure of information for certain purposes.

6.5 Common Law: - where there is a pressing social need to do so, it is necessary and proportionate, and the public interest outweighs the duty of confidentiality.

Section 7 Fairness and Transparency

7.1 The Data Protection legislation requires that personal data be processed lawfully, and fairly and in a transparent manner in relation to the data subject. It is the responsibility of all signatories to this Protocol to ensure that their privacy or fair processing notices properly reflect their data sharing arrangements. It is essential that signatory organisations have also paid the necessary fee to the Information Commissioner as required under the Data Protection Act 2018.

7.2 The signatories to this Protocol will be open and act in good faith in their dealings with each other.

7.3 This Protocol and, any Tier 2 Agreements arising from it, will normally be considered as suitable for both internal and external publication.

Section 8 What data is necessary to exchange?

8.1 Each organisation may have its own criteria or restrictions around what data may be provided in certain circumstances, which is a matter for them to consider on each occasion and cannot be prescribed in a document such as this.

8.2 In the case of personal data, the Data Protection Act 2018, the UK GDPR and the Human Rights Act 1998 apply and must be considered at every opportunity. As a general rule there must always be a clear purpose and a relevant legal gateway, and any data provided must be necessary, relevant, proportionate, the minimum necessary to achieve the purpose, and clearly distinguish fact from opinion. This means that even when there is a legal basis to share, it may not be appropriate to share all of the information requested. Every request should be dealt with on a case by case basis.

8.3 When personal data is shared an audit trail record must be retained of the request, what was shared and when, the reason for sharing and the authority to share, in case of a challenge, complaint or review. This will normally be captured in the Tier 2 Agreement.

8.4 It is important to note that shared data should only be used for the intended purpose, unless with the specific agreement of the originating organisation. It is also important that any shared data is held securely and not disclosed onwards without the original data controller being informed well in advance.

Section 9 Retention, Disposal and Security of Personal Data

9.1 Each agency should have retention and weeding policy(s) which they should follow unless otherwise agreed. In general terms, data should not be retained for longer than is required for the purpose for which it was supplied and needs to be retained, managed and eventually disposed of securely to avoid accidental and/or unauthorised alteration, deletion or disclosure. Every Tier 2 Agreement will have a retention period recorded which is specific to the information shared.

9.2 The security arrangements for the transmission, processing and retention of information shared, must comply with the Data Protection Act 2018 and the UK GDPR, be proportionate to the risk, adequately maintained and/or updated and in accordance with current good practice. Whilst ISO accreditation is not necessary, where appropriate, compliance should be aimed towards ISO/IEC27001 in respect of information management.

9.3 Data controllers agree to allow relevant signatory organisations, reasonable access to their premises to check[2] the arrangements for the retention, use, disposal and general security of the data shared by them.

Section 10 Data Quality

10.1 The originating agency is responsible for the quality of any data shared. Inaccurate information should not be shared. Information discovered to be inaccurate, not up to date or inadequate for the purpose, will be notified to the originating agency as soon as practicable. The originating agency will be responsible for correcting the data and notifying all other recipients, who in turn must ensure that their records are updated or amended. All agencies should endeavour, where practical, to work towards ISO 9001 (although accreditation to that standard is not necessary) and or apply relevant sector guidance/standards to the quality of their data.

Section 11 Training

11.1 Each partner is responsible for ensuring that relevant members of staff, including temporary and contract staff, are adequately trained in respect of all matters covered in this document and within appropriate Tier 2 ISAs.

Section 12 Complaints and Breaches

12.1 Any complaint and/or breaches made will be brought to the attention of the nominated officer appointed to manage data protection matters on behalf of the data controller of the relevant partner organisation, without delay. These will be dealt with in accordance with the respective organisational policies, procedures and legislative requirements. In particular it may be necessary to inform the Information Commissioner and the data

[2] ICO: Data sharing code of practice

subject of the breach without undue delay where the rights and freedoms of the data subject have been adversely affected.

12.2 Where there has been a data breach of data protection legislation, the relevant signatory organisation will provide all reasonable, timely and necessary assistance to the respective data controller(s) and the Information Commissioners Office, in order to help manage the breach, prevent further data losses, minimise harm to a data subject and maintain public confidence.

12.3 If a complaint is received in relation to the sharing of information under this Protocol, the respective signatories will keep each other informed of any developments, progress and lessons learned.

Section 13 Responsibilities of Receiving Organisation

13.1 Information shared becomes the responsibility of the receiving organisation. There is a clear expectation that the receiving organisation will manage the information received in accordance with the duties of a data controller, the Data Sharing Code of Practice the requirement of this is Protocol and related Tier 2 Agreements.

Section 14 Access Rights

14.1 The data subject and the general public have the right to ask to see information associated with these agreements and/or the specific personal data exchanged under any of them. The right to ask is assigned from both the Data Protection and Freedom of Information Acts.

14.2 Each signatory organisation will deal with such requests in accordance with their local arrangements. Where a request involves data belonging to another organisation, the receiving organisation shall contact the owning organisation to advise them accordingly and seek any representations, including whether, for example, an exemption applies under the Act. However, the decision to disclose rests with the receiving organisation.

Section 15 Closure / Termination of this Protocol

15.1 Each signatory organisation shall at all times maintain the security and integrity of all personal data supplied pursuant to this Protocol. This clause shall survive termination of the Agreement or the withdrawal of or removal of any signatory organisation.

15.2 This Protocol will be reviewed every two years. In the event of it being terminated, withdrawn or ceasing to have effect, the Avon and Somerset Constabulary, who host it, will write to all other signatories, giving at least 30 days' notice.

15.3 A signatory organisation can withdraw from this Protocol after giving 30 days' notice to the Avon and Somerset Constabulary. In the event of a withdrawal any associated Tier 2 Agreements would cease to have effect after the 30 day notice period.

15.4 A signatory organisation can be suspended from this Protocol following a major breach of the Data Protection Act or a breakdown in trust, for example. A suspension is likely to be a rare event and will be subject to a Risk Assessment and Resolution meeting. This panel will be made up of the signatories of this agreement, or their nominated representatives. A meeting will take place within 14 days of any suspension. Any associated Tier 2 Agreements will also be suspended accordingly and all reasonable steps must be taken to ensure that no further information is shared under this Protocol or related Tier 2 Agreements during the period of suspension.

15.5 It is important to note that the temporary suspension or withdrawal from this Protocol does not preclude the continued adhoc sharing of information with the affected partner if a legal gateway exists. A decision to share information will be made on a case by case basis.

15.6 The premature termination of a Tier 2 Agreement before its agreed expiry date should be in writing and will normally take immediate effect.

15.7 In the event of a suspension, withdrawal or termination of this Protocol and related Tier 2 Agreements, it is incumbent on the relevant parties to withdraw them from within their respective organisations and public facing sites as soon as practicable, and to communicate the fact to staff, interested parties and the wider public as appropriate.

Section 16 Nominated Host

16.1 The nominated host of this Protocol is the Avon & Somerset Constabulary Data Protection Officer (Compliance), who shall on behalf of the partner agencies:

- Ensure that a review is carried out biennially.
- Facilitate the circulation of all requests for change, co-ordinate responses, obtain agreement for the changes from the signatories to this Agreement and distribute up-dates as these become available.

Section 17 Signatures

17.1 By signing this document the participant(s) accept the statements, agree to maintain the specified standards, and commit to achieving compliance with any legal obligations.

Signed and dated:

Name:

Position:

Organisation name: