WARWICKSHIRE COMMUNITY SAFETY

INFORMATION SHARING PROTOCOL

JOINT APPROACH TO MAKE WARWICKSHIRE A PLACE WHERE PEOPLE FEEL SAFE TO LIVE, WORK, AND VISIT

COMMISSIONED BY THE SAFER WARWICKSHIRE PARTNERSHIP BOARD

September 2019

Updated June 2025

Contents

Page 3	Section 1	Introduction
Page 4	Section 2	Purpose of Information Sharing
Page 5	Section 3	Who Will Be Sharing Information?
Page 6	Section 4	What Is To Be Shared?
Page 7	Section 5	Fairness and Transparency
Page 8	Section 6	Arrangements for Data Sharing Within Multi-Agency Meetings
Page 9	Section 7	Process for Data Sharing Outside Meetings
Page 10	Section 8	Nominated Representatives
	Section 9	Data Controller Responsibilities
	Section 10	Agents and Sub-Contractors
	Section 11	Complaints
Page 11	Section 12	Non-Compliance and Partner Disagreement
	Section 13	Data Breaches
Page 12	Section 14	Retention and Disposal
	Section 15	Access to Information and Mutual Assistance
Page 13	Section 16	Monitoring and Review
	Section 17	Indemnity
Page 14	Section 18	Change History
	Section 19	Effective Date
Page 15	Appendix 1	Legal Basis for Sharing Information
Page 16	Appendix 2	Do We Need This Information?
Page 17	Appendix 2a	Flowchart of when and how to share information
Page 18	Appendix 3	Generic confidentiality declaration sign-in sheet
Page 20	Appendices 4-10	Specific confidentiality declarations / statements (One per setting in which data needs to be shared and a specific agreement or statement is used)
Page 32	Appendix 11	Request from external agencies to the Police for information
Page 35	Appendix 12	Request from the Police to external agencies for information
Page 39	Appendix 13	**Safer Warwickshire Partnership Board Signatures**
Page 42	Appendix 14	**Additional Signatures**

1. Introduction

1.1 **The Safer Warwickshire Partnership Board aims to create safer communities through the reduction of crime and the promotion of safety.**

1.2 The Board is responsible for putting in place an information sharing protocol to facilitate information sharing between responsible authorities for community safety in Warwickshire as required by the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007 (Regulation 4). This should be agreed by all responsible authorities, statutory agencies and other groups providing community safety in the county ("Partner agencies").

1.3 Responsible authorities as detailed by the **C**rime and **D**isorder **A**ct **1998**:

- The council for the area (County and District/Borough)
- Chief Officer of Police
- Probation Service
- Fire and Rescue Authority
- Integrated Care Board

1.4 The purpose of this information sharing protocol is to facilitate the secure sharing of information, including sensitive or confidential information, between partner agencies in Warwickshire; govern the secure use and management of information and enable partner agencies to meet their legislative obligations. Information sharing protocols such as this one have no statutory basis and do not substitute for appropriate controls within individual organisations when requesting, disclosing, and transmitting personal data, or the need for specific information sharing agreements where applicable. They do, however, demonstrate cooperation between partners and the intent to share information securely and effectively.

1.5 This information sharing protocol provides specific details for information sharing within a community safety context. As well as setting out the general principles to be followed when sharing community safety information, it includes (as appendices) confidentiality declarations for each specific multiagency meeting where data needs to be shared. Additional appendices are added as new groups or scenarios in which information needs to be shared emerge.

1.6 The settings currently covered in this protocol are as follows:

- *Using the generic confidentiality declaration (**see appendix 3**):*
  - Community Impact Operational Groups
  - Vulnerability meetings
  - Partnership Problem Solving meetings
  - Domestic Abuse Related Death Review Panels
  - Hate Crime meetings
  - ASB, Youth, Victim, Perpetrator, and other Case Management meetings
- Multi Agency Public Protection Arrangements (MAPPA) (***see Appendix 4***)
- Multi Agency Risk Assessment Conferences (MARAC) (***see Appendix 5***)
- Integrated Offender Management (IOM) Multi Agency Case Conferences *(**See Appendix 6**)*
- Local Contextual Safeguarding Meetings (***see Appendix 7***)
- Channel Panel (***see Appendix 8**)*
- Serious and Organised Crime Joint Action Group (SOCJAG) *(**see Appendix 9**)*
- Domestic Abuse Perpetrator Programme Panels (***see Appendix 10***)
- Community Safety Partnership meetings

1.7 Each partner must ensure compliance with applicable Data Protection legislation at all times during the term of this protocol.

2. Purpose of Information Sharing

2.1 The purpose of this protocol is to facilitate the lawful exchange of information, other than anonymised information, in order to comply with the statutory duty placed on the responsible authorities (as at 1.3 above) to work together to formulate and implement strategies for reducing crime and disorder (including anti-social behaviour and other behaviour); combatting the misuse of drugs, alcohol and other substances; reducing re-offending; preventing people from becoming involved in serious violence, and reducing instances of serious violence.

2.2 This protocol will also extend to co-operating organisations and any other agency or organisation which is a signatory to the document.

2.3 Information sharing is the cornerstone of delivering shared understanding of issues and arriving at holistic solutions. Effective delivery relies on good decision making and those decisions should be based on good information. The right information enables partners to carry out evidence-based, targeted community safety interventions and evaluate their impact. The improved outcomes of an intelligence led, problem solving approach to community safety can only be achieved when partners have access to relevant, robust, and up-to-date information from a broad range of sources.

2.4 Partners should also consider the likely effect of not sharing information, for example, harm to individuals, damage to their organisations' reputation, a disconnect in partnership working and lack of understanding of problems.

3. Who Will Be Sharing Information?

3.1 Partners who are required to share information are named as the responsible authorities in the Crime and Disorder Act 1998, as amended. These are the council for the area (*including County and District/Borough*), Probation Service, Chief Officer of Police, Fire and Rescue Authority, and the Integrated Care Boards.

3.2 Persons or bodies may 'co-operate' in the exercise of responsible authorities' functions, including sharing information. "Co-operating persons and bodies" include Parish Councils, School and College Governing bodies, Registered Social Landlords, and agencies appropriate to the location or circumstances.

3.3 Various other bodies may 'participate' in the exercise of responsible authorities' functions. "Participating persons and bodies" may also be asked to share information.

3.4 Wider partners may also be required to share information in specific circumstances. These could include schools, other health agencies and voluntary sector organisations.

3.5 Collectively, these organisations shall be referred to as "Partner agencies". This protocol is approved by the Safer Warwickshire Partnership Board. Member organisations of this Board sign up to the principles of the protocol by virtue of their membership. Other partners can formally sign up to the protocol. To do so, or to check if an agency has signed up to the protocol, please email communitysafety@warwickshire.gov.uk.

3.6 Where an agency is not signed up to the protocol, but a partner/partners wish to share Personal Data with them, extra care should be taken to ensure they understand how sensitive information they see should be shared and handled by providing a specific instruction and handling arrangement and ensuring the agency representatives sign a confidentiality agreement to confirm that they understand their responsibilities. **A generic agreement for this can be found at Appendix 3.** Where appropriate, a Data Protection Impact Assessment (DPIA) should be completed before any information is shared.

4. What Is 'To Be Shared'? (Referred to as "Shared Personal Data")

4.1 The 'Delivering Safer Communities' guidance and the Crime and Disorder Act 1998 place a duty upon relevant authorities to share information. Additionally, partner agencies have express and/or implied powers to share information as set out in legislation. (See **Appendix 1** for a list of legislation. Note that this is not an exhaustive list)

4.2 Shared Personal Data will usually include information about the nature of the problem and, where relevant, personal data such as names, addresses and dates of birth of offenders, victims, or witnesses.

4.3 Most of the Shared Personal Data will also include sensitive/special category/criminal offence personal data as defined in data protection legislation. Sharing of this type of sensitive information is allowed in lawful and appropriate circumstances. Any sharing of personal data including sensitive data known as special category data or criminal offence data must be undertaken in accordance with UK GDPR and the Data Protection Act (DPA) 2018. Relevant sections of the legislation enabling lawful data sharing include but are not limited to:
- UK GDPR Article 6(1)(d): Protection of vital interests of the subject or another person
- UK GDPR Article 9(2)(g): Reasons of substantial public interest (with a basis in law)
- DPA Schedule 1 Part 2 Paragraph 10: Preventing or detecting unlawful acts
- DPA Schedule 1 Part 2 Paragraph 18: Safeguarding of children and individuals at risk
- DPA Schedule 2 Part 1 Paragraph 2: Crime and taxation: general.

4.4 In order to share appropriate information between partners there must be a lawful, defined, and justifiable purpose(s) which supports the effective delivery of a policy or service that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This protocol is supplemented by a number of questions, included at **Appendix 2**, designed to 'walk' Managers/Designated Persons and other specialist support through a process to assess the impact and appropriateness of information sharing.

4.5 'Signatories' to this protocol understand that Shared Personal Data will be shared at multi-agency meetings (see **Section 6**). For example, there may be meetings between members of staff from different agencies sharing information about a common case to build a foundation of accurate knowledge and evidence, to minimise the risk of harm to the community, whilst allowing proper management of the case. As well as meetings, the protocol also covers other forms of information exchange such as electronic information sharing. The intention of this protocol is to cover all such information sharing provided the safeguards described within it are followed.

4.6 If any Shared Personal Data relates to an ongoing investigation or prosecution by any of the agencies then consultation must take place with the investigating officer and Crown Prosecution Service as the matter will be sub-judice. This will ensure that disclosure will not adversely prejudice the outcome of the matter.

4.7 Special care should be taken when considering the sharing of information that could constitute profiling, particularly of children or minority groups. A lawful basis must be available and DPIA prepared before any sensitive information is shared.

4.8 More information about information sharing is available from the Information Commissioner. Go to https://ico.org.uk/

5. Fairness and Transparency

5.1 In the interests of fairness and transparency, partners agree to the following principles:

5.2 All information will be shared in a lawful manner. Any Shared Personal Data, including special category data and criminal offence data will be shared lawfully and in accordance with the data protection principles, UK GDPR and Data Protection Act 2018.

5.3 Data protection principles require individuals to make sure personal information is:

- used fairly, lawfully, and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant, and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage.

5.4 Where possible, anonymised or aggregated statistical information will be used.

5.5 Where appropriate, safe and possible, individuals will be requested to provide their 'agreement to share' with appropriate partner agencies. This consent will be secured in accordance with the standards set out in the UK GDPR

5.6 Where it is not appropriate to seek informed consent, personalised information will only be shared if there is another lawful basis to share it under data protection legislation or, where relevant, one of the exemptions in the Data Protection Act 2018 (see paragraph 4.3) applies. The questions listed at Appendix 2 help to assess the impact on service users of decisions relating to information sharing.

5.7 Information Sharing Agreements will be developed and/or DPIAs undertaken for each purpose or scenario in which different types of personal data will be shared, including new purposes or scenarios as they arise. It is recommended that partner agencies shall be responsible for the completion and updating of the Information Sharing Agreements / DPIAs for each meeting and data sharing scenario they deliver.

5.8 Each organisation will have a nominated Data Protection Officer to oversee their information sharing responsibilities and will be correctly registered with the Information Commissioner to share appropriate information.

5.9 Partner agencies shall be responsible for updating their privacy notices to provide details of information sharing and to inform individuals about the processing of their data.

6. Arrangements for Data Sharing Within Multi-Agency Meetings

6.1 Using the definitions in 6.4 of this protocol the chair of each meeting should designate the level of confidentiality appropriate to the information being shared at the outset and, where relevant, provide a confidentiality declaration sign-in sheet (**Appendix 3**) which states the data sharing requirements relevant to the meeting. If used, the chair should securely retain a copy of this confidentiality declaration sign-in sheet.

6.2 The parties to this protocol understand that in keeping with government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the Crime and Disorder Act 1998, it is likely that there will be individuals present at certain meetings who are not representing an organisation which is a signatory to this protocol. To allow for this, the signing-in sheet should state that the signatory agrees to abide by all the terms of this protocol.

6.3 It is good practice to use the Government Security Classifications. These set out levels of confidentiality and appropriate security measures. These classifications are the method by which the originator of an asset (that is all material assets, i.e., papers, drawings, images, disks, and all forms of electronic data records) indicates to others the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within the guidance and outside the originator's own department or force and its ultimate method of disposal.

6.4 The levels of classification are:

OFFICIAL - all routine public sector business, operations, and services.

OFFICIAL – SENSITIVE - a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen, or published in the media. In cases where there is a clear and justifiable requirement to share only on a need-to-know basis, the OFFICIAL–SENSITIVE classification should be used.

SECRET – Very sensitive information where compromise would directly threaten an individual's life, liberty or safety or cause serious damage to the effectiveness or security of the UK.

TOP SECRET - Exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies.

6.5 The chair of each multiagency meeting is responsible for ensuring the confidentiality declaration sign-in sheet is kept current and, as far as they are able to, includes all legal requirements surrounding information sharing.

7. Process for Data Sharing Outside Meetings

7.1 This protocol has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be lawful and justified on the merits of each case.

7.2 Information must be requested in a legally compliant manner, setting out the legal grounds for disclosure. For example, if the Crime and Taxation exemption under the DPA 2018 Schedule 2 Part 1 (2) is being relied on, then this should be formally set out and the specific details provided. Where relevant, including the use of information as evidence for prosecution, the Warwickshire Police access request forms (**Appendices 11 and 12**), or alternative official third-party subject access request form where required by other partners, must be used.

7.3 Partners sharing information should make clear who the information can be shared with in their Privacy Notice and Record of Processing Activity (ROPA). Information shared should only be used for the purpose requested by the requesting partner and should not be shared further without consent of the information owner unless there is a legal obligation or other lawful basis for doing so.

7.4 Any data should be shared and stored in accordance with the relevant legislation. In particular, where the data to be shared is personal, a secure transmission system should be used, such as secure email (or standard email systems where these are confirmed to be secure[1]), courier or hosted on a secure system shared by partners. All partner agencies must have appropriate technical and organisational measures in place, having regard to the nature and sensitivity of the information, to ensure information security. This will include monitoring and auditing procedures as well as the ability to respond to any failure to adhere to the data sharing protocol swiftly and effectively and to report any personal data breach.

7.5 It is the responsibility of each partner to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data. Shared Data shall be accessible only to personnel who require access for the purposes outlined in this protocol and partners must ensure access controls are in place.

7.6 Any information shared should only be kept as long as it is necessary and then confidentially destroyed by all signatories in accordance with any relevant data retention and disposal policies.

7.7 **Appendix 2** gives a checklist to help ensure that data is lawfully shared.

[1] The following email suffixes for statutory bodies are known to be secure: gov.uk, justice.gov.uk, police.uk, nhs.net, cjsm.net.

8. Nominated Representatives

8.1 Each partner organisation shall have a Designated Officer who will facilitate data sharing under this protocol where issues arise.

8.2 Any disputes or disagreements between parties, including why one agency decides not to share information with another, shall be resolved by discussion between the Designated Officers if at all possible, or between the heads of each agency.

9. Data Controller Responsibilities

9.1 Data Controllers must make appropriate notifications of any data breaches to the Information Commissioner in compliance with the UK GDPR and in accordance with any guidance issued by the Article 29 Working Party and the Information Commissioner's Office. This notification should include details of the Data Protection Officer or nominated contact.

10. Agents and Sub-Contractors

10.1 Each partner organisation shall ensure its agents and sub-contractors comply with the provisions of the protocol.

11. Complaints

11.1 Each partner organisation will deal with the complaints in accordance with their own procedures, which will ensure that:

- Service users are aware that they can complain and of how to go about it;
- Complaints are acknowledged promptly in writing;
- The complaint is investigated fairly and thoroughly;
- Service users are given an appropriate written response;
- If appropriate the appeals procedures are explained to the service user.

11.2 If two or more partner organisations receive a complaint about the same matters, they should investigate and respond to the complaint jointly.

11.3 If a partner organisation receiving a complaint believes another partner organisation may be responsible, wholly, or partly, for the matters complained of it should notify the other organisation and the organisations should investigate and respond to the complaint jointly.

11.4 In the event of a dispute, complaint or claim brought by a Data Subject or the Information Commissioner (ICO) concerning the processing of Shared Personal Data against one or more partners, the partners will inform each other about any such disputes, complaints or claims, and will cooperate with a view to settling them amicably in a timely fashion.

11.5 The partners agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the ICO. If they do participate in the proceedings, the partners may elect to do so remotely (such as by telephone or other electronic means). The partners also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

11.6 Each party shall abide by a decision of a competent court of the Data Discloser's country of establishment or of the Information Commissioner or a Supervisory Authority.

12. Non-Compliance and Partner Disagreement

12.1 In the event of a suspected failure within their organisation to comply with this protocol, partner organisations will ensure that an adequate investigation is carried out and recorded. If the partner organisation finds there has been a failure it will ensure that:

- Necessary remedial action is taken promptly;
- Service users affected by the failure are notified of it, the likely consequences, and any remedial action;
- Partner organisations affected by the failure are notified of it, the likely consequences, and any remedial action.

12.2 If one partner organisation believes another has failed to comply with this protocol it should notify the other partner organisation in writing giving full details. The other partner organisation should then investigate the alleged failure. If it finds there was a failure, it should take the steps set out above. If it finds there was no failure it should notify the first partner organisation in writing giving its reasons.

12.3 Where it is clear that a partner organisation is not complying with this protocol, other partners may decide to stop sharing information until the issues are resolved.

12.4 Partner organisations will make every effort to resolve disagreements between them about personal information use and sharing. However, they recognise that ultimately each organisation, as Data Controller, must exercise its own discretion in interpreting and applying this protocol and ensuring compliance with the data protection legislation.

12.5 Nominated representatives should be notified at an early stage of any suspected or alleged failures in compliance or partner disagreements relating to their organisation.

13. Data Breaches

13.1 A data breach is where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Where there has been a data breach by or on behalf of a partner in respect of any Shared Personal Data, the partner agency where the data breach has occurred will inform all affected partners of the data breach immediately to enable them, where relevant, to meet their legal duty under UK GDPR to report personal data breaches within 72 hours.

13.2 The partner agency needs to take immediate action to recover the information, if safe to do so.

13.3 The partner agency where the breach has occurred shall conduct a full investigation of the breach using its own procedures and systems and the findings of the investigation will be shared with the other partners and the Safer Warwickshire Partnership Board. All partner agencies affected will provide mutual assistance to the lead partner where required for the investigation.

13.4 Partners need to formally record all data breaches in respect of personal data they are data controller in respect of, internally within their organisation and inform the Safer Warwickshire Partnership Board to ensure effective monitoring and reviews can take place.

14. Retention and Disposal

14.1 Partners must comply with their own agencies' retention and disposal policies. These should cover both electronic and paper-based information.

15. Access to Information and Mutual Assistance

15.1 Partners must have in place policies to deal with people's information rights under Freedom of Information (FOI) legislation, UK GDPR and the Data Protection Act (DPA) 2018.

15.2 Each partner agency shall assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

- consult with the other partners about any notices given to data subjects in relation to the Shared Personal Data;
- promptly inform the other partners about the receipt of any data subject access request;
- provide the other partners with reasonable assistance in complying with any data subject access request;
- not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the other partner wherever possible;
- assist the other partner, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- notify the other partner without undue delay on becoming aware of any breach of the Data Protection Legislation;
- at the written direction of the Data Discloser, delete or return Shared Personal Data and copies thereof to the Data Discloser on termination of this agreement unless required by law to store the personal data;
- use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers; and
- maintain complete and accurate records and information to demonstrate its compliance with this clause.

16. Monitoring and Review

16.1 The Safer Warwickshire Partnership Board will annually monitor and review the contents and implementation of this Information Sharing Protocol. The review will have regard to:

- Changes in the relevant law and statutory or other government or national guidance;
- Service user and staff opinions, concerns, and complaints;
- Failures in compliance and disagreements between partner organisations;
- Any other relevant information.

17. Indemnity

17.1 Each partner shall indemnify the others against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified partner arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying partner, its employees or agents, provided that the indemnified partner gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

18. Change History

Version	Amended by	Amended date	Summary of main changes
Draft v0.1	Katie Whitehouse	19/01/2018	Reviewed entire protocol agreed in December 2013. Updated in light of changes to legislation, regulation, and policy.
Drafts v0.2 – 0.8	Katie Whitehouse, Alex Gloster, Cheryl Bridges	20/02/2018 – 09/09/2019	Updated to include feedback and additional information from partner agencies.
Annual update 2020	Cheryl Bridges	09/12/2020	Reviewed and added an additional appendix
Annual update 2021	Cheryl Bridges/Katie Whitehouse	15/10/2021	Reviewed, minor updates to the text to reflect partner feedback and new legislation, checked and updated all appendices, listed meetings to use generic confidentiality declaration
Annual update 2021	Katie Whitehouse	07/12/2021	Updated based on feedback received at SWPB meeting to reflect position regarding the recording virtual meetings and status of the OPCC.
Annual update 2022/3	Stephen Croshaw	12/07/2023	Reviewed and updated re current legislation, checks with partners and staffing amendments as known at this time.
Annual update 2024	Stephen Croshaw / Katie Whitehouse	08/05/2024	Reviewed and updated, minor updates to text to reflect partner feedback and contact details as known at this time. Additional signatories appendix listed in alphabetical order.
Annual update 2025	Katie Whitehouse / Laura Evans	05/06/2025	Reviewed and updated. Updates made to text to reflect partner feedback, contact details and legislation changes as known at this time. Review undertaken by Warwickshire County Council Information Governance and Legal Services and amendments incorporated. Meeting confidentiality declaration appendices updated where required. Contact details for additional signatories checked.

19. Effective Date

19.1 This protocol is effective from an agreed common implementation date of 1st August 2019 and will be subject to an annual review as shown in the table above to ensure it remains current and relevant.

Appendix 1 – Legal Basis for Sharing Information

There are a considerable number of Acts and Regulations that require or enable the sharing of information in respect of crime and disorder, including:

- **Children Act 1989 and 2004**
- **Housing Act 1996**
- **Human Rights Act 1998**
- **Crime and Disorder Act 1998, and the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007 made under the Act**
- **Criminal Justice and Court Service Act 2000**
- **Sexual Offences Act 2003**
- **Criminal Justice Act 2003**
- **Domestic Violence Crime and Victims Act 2004**
- **Offender Management Act 2007**
- **Police and Justice Act 2006, and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 made under the Act**
- **Policing and Crime Act 2009**
- **Police Reform and Social Responsibility Act 2011, and the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2012 made under the Act**
- **Legal Aid, Sentencing and Punishment of Offenders Act 2011**
- **Crime and Courts Act 2013**
- **Care Act 2014**
- **Anti-Social Behaviour, Crime and Policing Act 2014**
- **Offender Rehabilitation Act 2014**
- **Counter Terrorism and Security Act 2015**
- **Serious Crime Act 2015**
- **Modern Slavery Act 2015**
- **Policing and Crime Act 2017**
- **General Data Protection Regulation 2018**
- **Data Protection Act 2018**
- **Domestic Abuse Act 2021**
- **Police, Crime, Sentencing and Courts Act 2022, and the Prevention and Reduction of Serious Violence (Strategies etc.) Regulations 2022 made under the Act**
- **Victim and Prisoners Act 2024**
- **Terrorism (Protection of Premises) Act 2025**

Appendix 2 – Do We Need This Information?

1. Why do I want the information? Is sharing this information in the best interests of the victim, offender, or vulnerable individual (1)?

2. Is there a sufficient need to know? If the information is shared will this make a difference to the service offered and to the outcomes for the victim, offender, or vulnerable individual? Is it necessary for me to do my job or to fulfil a statutory duty?

3. Are the reasons for the request "proportionate" for the purpose e.g.

    - Are the reason or reasons for sharing information justifiable under Article 8 of the Human Rights Act?
    - Can less information be shared and still achieve the best interest of the victim, offender, or vulnerable individual?
    - Is there another equally effective way of achieving the same aim? Can I share less information and still achieve the best interest of the victim, offender, or vulnerable individual.
    - What is the impact of disclosure likely to be on the individual?
    - If the information requested is sensitive information (race or ethnicity, political or religious beliefs, health, sexual life, criminal offences, trade union membership), is it necessary to share this to meet the reason for sharing?

4. Is the information up to date and accurate? (Care should be taken when recording the name, date of birth and address to ensure that when data is merged from different agencies it relates to the same person).
   Also do I distinguish between fact and opinion or judgement?

5. Will the request involve secondary disclosure and if so do I need to check with the person who told me this information or wrote this report before I share it?

6. Have I got consent? If so is it recorded on a file or is there a consent form, are there any restrictions?

7. On the assumption that the consent cannot realistically be obtained or sought, is there a lawful basis for sharing without consent, e.g., to protect the interests of the victim/offender?

8. Have I recorded that I have shared this information?

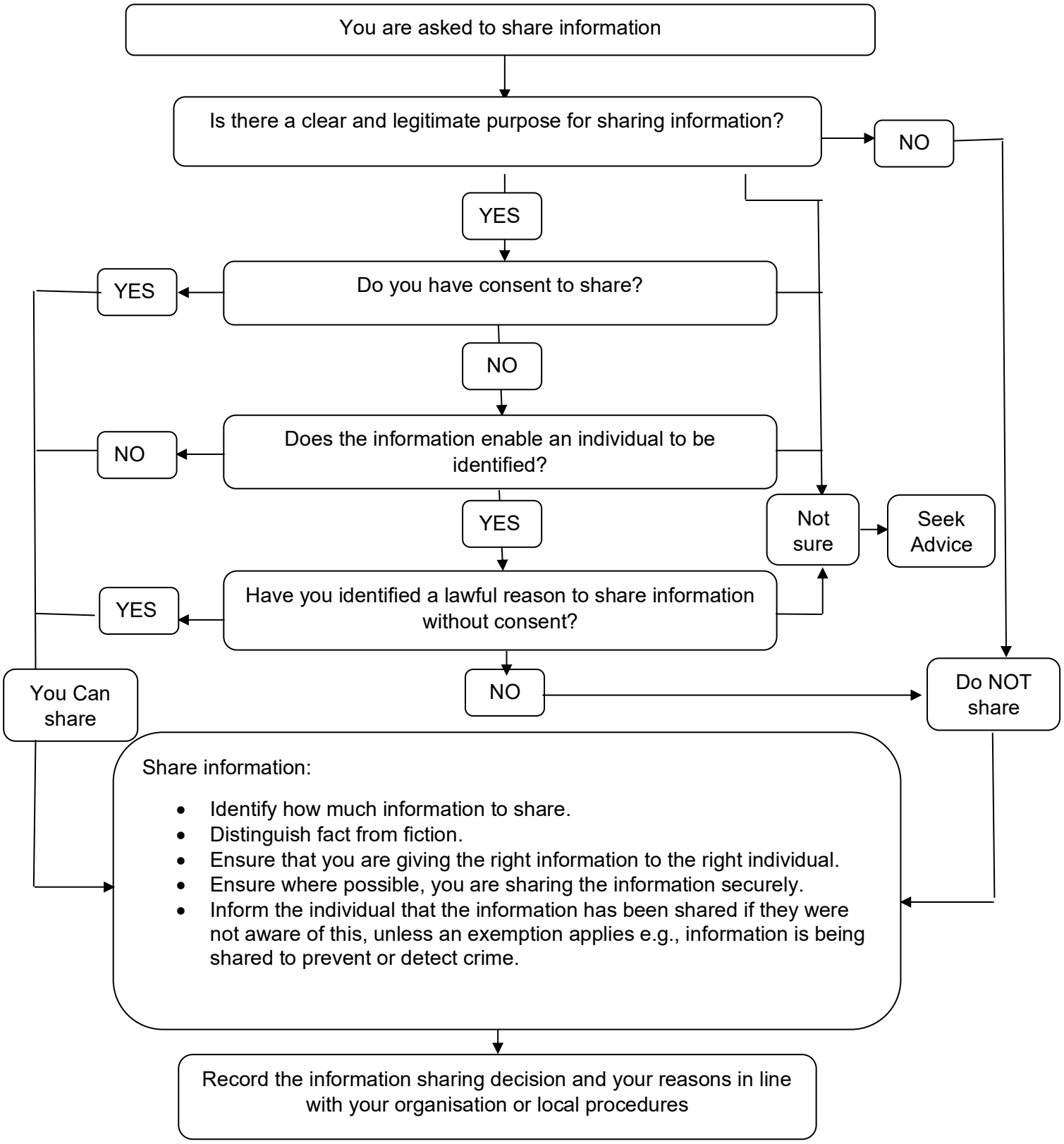
9. Am I sharing this information in a secure way?

10. Have I recorded this information in the relevant system(s)?

(1) *A vulnerable individual for the purpose of this information sharing protocol is taken from the College of policing definition:*

- *A person is vulnerable if, as a result of their situation or circumstances they are unable to take care of, or protect themselves or others, from harm or exploitation.*

Flowchart of when and how to share information. *From HM Government Information sharing July 18*



If there are concerns that a child or vulnerable adult is in need, suffering or likely to suffer harm, then follow the safeguarding procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the decision is recorded.

Consent must be unambiguous, freely given and may be withdrawn at any time.

Appendix 3 – Generic confidentiality declaration sign-in sheet

Confidentiality Declaration[2]

****OFFICIAL-SENSITIVE****

Name of meeting:

Chair: **Date of meeting:**

Purpose of the meeting:

Any personal information or sensitive personal information known as special category data disclosed to you during this meeting has been provided to you in strict confidence and for the purpose of:

1. The detection of crime and anti-social behaviour
2. The prevention of crime and anti-social behaviour
3. The apprehension of an offender for crime or anti-social behaviour
4. The prosecution of an offender for crime or anti-social behaviour

Subject to Section 115 Crime and Disorder Act 1998, the General Data Protection Regulations 2016/679, and Data Protection Act 2018 in particular exemptions to UK GDPR set out at Schedule 2 Part 1 Section 2 Data Protection Act 2018.

- The information shared is done so on a lawful basis. The lawful basis relied upon is to perform a task in the public interest. The lawful basis for processing special category data is in the substantial public interest for the administration of justice. Information should only be shared on a need-to-know basis and must not be disclosed to any third party, including the data subject and other staff who do not have direct involvement in the original purpose for which it was disclosed. Further dissemination will only be permitted where there is a lawful basis to do so.
- It must be stored securely and permanently deleted when it is no longer required for the purpose for which it is provided.
- Any Warwickshire Police information shared is only valid at the time of provision and should only be used for the purpose as disclosed. It is only disclosed for the specific purpose given at the time of disclosure and should not be used for any other purpose.
- Any information shared will be proportionate and necessary for the purpose for which it is being shared.
- Where possible information shared must be handled and stored in accordance with the Government Protective Marking Scheme.
- Where personal information is shared with organisations that do not have access to secure email addresses, it must be encrypted with a password.
- Attendees joining the meeting virtually must ensure that confidentiality is maintained throughout.
- Due consideration will be given to the implications of recording the meeting and how this could be used, and agreement sought from all attendees before any recording commences.

[2] Agreed for use in Community Impact Operational Groups, Vulnerability meetings, Partnership Problem Solving meetings, Domestic Abuse Related Death Review Panels, Hate Crime meetings, Stratford District ASB and Case Management meetings, Warwick District ASB and Case Management meetings, Rugby Borough ASB Youth and Victim Case Management meetings, Nuneaton and Bedworth Borough ASB meetings and North Warwickshire Borough ASB meetings.

- All persons signing this document are duly authorised to act on behalf of their respective organisation to adhere to the conditions set out.

Please note, by signing this sheet you are agreeing to comply with the requirements of the Safer Warwickshire Partnership Board Community Safety Information Sharing Protocol and/or the specific Information Sharing Protocol applicable to this meeting.

Name	Signature	Organisation Represented

Appendix 4 – MAPPA Confidentiality & Equality Statements

MAPPA
Multi Agency Public Protection Arrangements

CONFIDENTIALITY STATEMENT

In working with offenders, victims and other members of the public, all agencies have agreed boundaries of confidentiality. The information contained in these MAPPA meetings respects those boundaries of confidentiality and is shared under an understanding that:

1) The meeting is called in circumstances where it is felt that the risk presented by the offender is so great that issues of public or individual safety outweigh those rights of confidentiality.

2) One or more of the following exemptions will probably apply to the minutes of the meeting under the Freedom of Information Act 2000:

   a) Investigations and proceedings by Public Authorities (s.30(1)(B));
   b) Health and safety (s.38);
   c) Personal information (s.40);
   d) Information provided in confidence (s.41).

3) Where no exemptions apply, an individual's own personal data will be released to them if they make a Subject Access Request under the Data Protection Act 2018.

4) The discussions and decisions of the meeting will involve an interference with the offender's Article 8 rights to privacy and a private life. Such an interference must be justified on one of the following grounds that are found in Article 8.2 of the European Convention on Human Rights and be necessary and proportionate to the risk posed:

   a) Public safety;
   b) The prevention of crime and disorder;
   c) The protection of health and morals;
   d) The protection of the rights and freedom of others.

5) Where meetings are undertaken remotely, participants will ensure they are in an appropriate location where they cannot be overheard, including by smart speakers, and where their screens cannot be seen.

6) The minutes of the meeting will be marked Official-Sensitive. Minutes should be stored on ViSOR. Agency copies must be stored in line with individual agencies' policies on the retention of Official-Sensitive information. **Minutes must not be photocopied nor may the contents be shared outside of the meeting without the agreement of the meeting Chair.** Permission must be sought from the Chair if it is essential that information is shared with another agency. The Chair will then consult all those whose information is contained in the minutes and decide what information can be shared (information shared will be on a need-to-know basis and must be proportionate and necessary). Copies of minutes will not be taken to or from meetings.

DIVERSITY, INCLUSION AND EQUALITY STATEMENT

MAPPA meetings must promote equal access to services for all groups, ensuring that policies and procedures comply with Human Rights requirements and do not draw on stereotypical assumptions about groups of offenders or victims or contain any elements that will be discriminatory in outcome.

The meeting must consider

- if any of the nine protected characteristics set out in the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage & civil partnership, pregnancy & maternity, race, religion or belief, sex, sexual orientation) apply to the offender or the victim, and
- whether any other diversity issues may affect the offender or have a bearing upon the risks they present to others and how these can be managed.

Appendix 5 – MARAC Confidentiality Statement

WARWICKSHIRE AGAINST
DOMESTIC ABUSE

CONFIDENTIALITY DECLARATION: AS READ BY THE MARAC CHAIR

By accepting MARAC meeting outlook invite you are agreeing to the terms of the confidentiality statement and the Warwickshire Community Safety Information Sharing Protocol. The confidentiality agreement will be confirmed at the start of the meeting.

The purpose of the MARAC

MARAC is a multi-agency meeting that focuses on the safety of victims/survivors of domestic abuse identified as being at high risk for serious harm or homicide. The purpose of the MARAC is to:

- to share information to increase the safety, health and well-being of victims adults and their children;
- to determine whether the perpetrator poses a significant risk to any particular individual or the general community;
- to construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
- to reduce repeat victimisation;
- to improve agency accountability;
- improve support for staff involved in high risk DV cases; and
- the responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC it is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

Information sharing

Subject to Section 115 Crime and Disorder Act 1998, the General Data Protection Regulations 2016/679 and Data Protection Act 2018 in particular exemptions to GDPR set out at Schedule 2 Part 1 Section 2 Data Protection Act 2018. The information shared is done so on a lawful basis. The lawful basis relied upon is to perform a task in the public interest. The lawful basis for processing special category data is in the substantial public interest for the administration of justice.

Information shared at MARAC must be proportionate, relevant and necessary to enable an accurate assessment of the risks. A clear distinction should be made between fact and professional opinion.

Each MARAC agency is the data controller for the information which it brings to MARAC.

Attendance at the virtual MARAC meetings

A new dial in link will be circulated prior to each MARAC meeting to the approved list of MARAC representatives. Agencies must not forward the dial in details to any person without the prior consent of the MARAC Chair. When joining the meeting please enter your name and organisation when prompted, if you do not do so you will not be let into the meeting. During the calls, all attendees working from home must ensure that they attend the meeting in a room where no other people are present. If there are special circumstances, this should be dealt with by the Rep's manager and raised at Steering Group for approval.

WARWICKSHIRE AGAINST
DOMESTIC ABUSE

MARAC meetings must not be recorded. Virtual MARAC meetings will be held via Microsoft Teams– this does not allow participants to record the meeting, nor does it upload recordings to cloud. The MARAC Coordinator will hold people in the 'lobby' and approve members to meeting manually to ensure only relevant people are on the
call. No Guest agencies will be invited, without the consent of the MARAC Chair. Participants working from home must turn off and unplug any smart devices to ensure that MARAC meetings are not accidentally recorded. Should a participant become aware that a device has recorded the meeting, this must be brought to the attention of the Chair immediately.

All normal processes should be abided by, we must have trust that all Reps will continue to act within existing protocols to the best of their ability.

Observers at MARAC

Due to the highly sensitive information shared at MARAC, it is at the discretion of the MARAC Chair for observers to attend. Details of the proposed observer (full name and occupation) must be sent to the MARAC Coordinator two working days in advance of the MARAC meeting along with confirmation that there are no conflicts of interest with the observer attending. If the request is approved by the MARAC Chair, an invitation will be sent to the observer by the MARAC coordinator by email. The observer must confirm by email that they have read and understood the confidentiality statement ahead of the MARAC.

Storage of MARAC documents

All agencies should ensure that all minutes and related documentation are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to age, disability, gender reassignment, marriage and civil partnership, pregnancy, maternity, race, religion or belief, sex and sexual orientation.

All agencies must ensure home workers have secured all MARAC documents and it is not accessible to any household members. When emailing, only use secure (i.e. CJSM, Egress), or password protect. No passwords or automatic login should be saved on their home computer.

Disclosure of minutes

Information discussed by the agency representatives, within the ambit of this meeting, is strictly confidential and must not be disclosed to the victim, alleged perpetrator or any third parties who have not signed up to the MARAC ISP, without the agreement of the partners of the meeting. The procedure for requesting MARAC minutes is contained in the Warwickshire MARAC Operating Protocol.

All agency representatives understand that the MARAC minutes may need to be shared with another MARAC following the Warwickshire MARAC. This would only be as part of the MARAC to MARAC referral in line with the MARAC Operating Protocol. Should any agency representative have any concerns regarding this option for any case, then they should be raised and addressed during the case discussion.

WARWICKSHIRE AGAINST
DOMESTIC ABUSE

Confidentiality breaches

Any breaches must be immediately raised with MARAC Coordinator and Chair. This is not to place blame or punish, but rather to ensure we are adapting policies as needed in these new times to ensure confidentiality. We will explore how the breach occurred and determine if this is a one-off or systemic issue and respond accordingly. It is vital we remain open, transparent, and reflective with each other during this time while we shape this response plan.

Appendix 6 – Integrated Offender Management (IOM) Multi Agency Case Conference Confidentiality Declaration

IOM Multi Agency Case Conference

Statement of Confidentiality

By accepting the MACC meeting invite you are agreeing to the terms of the confidentiality statement and the Warwickshire Community Safety Information Sharing Protocol. The confidentiality agreement will be confirmed at the start of the meeting.

There is a requirement for all agencies in attendance to clearly understand that the details of what is discussed at the MACC meeting is of a sensitive nature and should only be recorded, discussed, or disseminated in the pursuit of crime reduction and via the means of appropriate data protection principles. Breaches will be dealt with in accordance with the Data Protection Act 1998.

Subject to Section 115 Crime and Disorder Act 1998, the General Data Protection Regulations 2016/679 and Data Protection Act 2018 in particular exemptions to GDPR set out at Schedule 2 Part 1 Section 2 Data Protection Act 2018. The information shared is done so on a lawful basis. The lawful basis relied upon is to perform a task in the public interest. The lawful basis for processing special category data is in the substantial public interest for the administration of justice.
Information shared at MARAC must be proportionate, relevant and necessary to enable an accurate assessment of the risks. A clear distinction should be made between fact and professional opinion.

Information discussed by the agency representatives, within this meeting, is strictly confidential and must not be disclosed any third parties without the agreement of the chair of the meeting.

Mission	IOM is a concept supported by the Home Office and the Ministry of Justice. Warwickshire will work together to provide an efficient and effective, multi-agency response to those offenders identified as subject to IOM, in order to secure sustainable reductions in offending, reducing its impact of victims and communities, and protect the public from crime.
VISION	We will operate in an open and transparent manner, facilitating internal and external challenge and scrutiny to create a culture of continuous improvement. We will co-ordinate our resources to: i) Increase public confidence in the CJS and contribute to making communities safer. ii) Target and investigate perpetrators, in order to bring them to justice and prevent re-offending. iii) Improve the IOM offender journey to provide a holistic package of interventions that is fully aligned and coordinated by the IOM scheme with a view to improving outcomes for this group of individuals and the communities in which they live.

N.B: Not transfer any Shared Personal Data received from another Partner Agency outside the UK

Appendix 7 – Local Contextual Safeguarding Meetings Confidentiality Statement

All participants must read and agree to adhere to the Local Contextual Safeguarding Group Confidentiality statement prior to participating in the meeting.

Information discussed by the agency representatives, within the ambit of this meeting, is strictly confidential and must not be disclosed to third parties who have not signed up to the Local Contextual Safeguarding Group, without the agreement of the partners of the meeting. It should focus on child protection concerns and a clear distinction should be made between fact and professional opinion.

All agency representatives understand that Local Contextual Safeguarding Group minutes may need to be shared with other agencies following the Operational Group. This would only be as part of a multi-agency referral to another safeguarding agency in line with the safeguarding operating protocols as set out by the WSP. Should any agency representative have any concerns regarding this option for any case, then they should be raised and addressed during the case discussion.

All agencies should ensure that all minutes and related documentation are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

Appendix 8 - Channel Panel Confidentiality Statement and Information Sharing

CONFIDENTIALITY STATEMENT
(Read at the start of each meeting)

"A reminder to Warwickshire Channel Panel members that you are all bound by the confidentiality of the Official Secrets Act and information must not be shared beyond this meeting. Please ensure when you join the meeting that you are in a space where confidentiality can be maintained. You must not record or screenshot any documentation that is shared on screen during this meeting."

Information Sharing and Storage

> **Key Principle:** Partners may consider sharing personal information with each other for *Prevent* purposes, subject to a case-by-case basis assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being necessary, proportionate and lawful.

The overriding principles for sharing information are necessity and proportionality. It should be confirmed by those holding information that to conduct the work in question it is necessary to share the information they hold. Only the information required to have the desired outcome should be shared, and only to those partners with whom it is necessary to share it to achieve the objective. Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an individual or the public. Consideration should also be given to whether discussion of a case is possible with anonymised information, for example, referring to "the young person" without the need to give the individual's name, address or any other information which might identify them.

The Warwickshire Community Safety Information Sharing Protocol provides the framework for Prevent information sharing, and specifically references Channel. Each case should be judged on its own merit, and the following questions should be considered when sharing information:

- what information you are intending to share
- to whom you are intending to pass the information
- why you are intending to pass the information (i.e. with what expected outcome)
- the legal basis on which the information is to be passed

The default should be to consider seeking the consent of the individual to share information. There will, of course, be circumstances in which seeking the consent of the individual will not be possible, because it will prejudice delivery of the intended outcome, and there may be gateways or exemptions which permit sharing to take place without consent. If you cannot seek or obtain consent, or consent is refused, you cannot share personal information without satisfying one of the gateway or exemption conditions. Compliance with the Data Protection Act (DPA) and Human Rights Act (HRA) are significantly simplified by having the

subject's consent. The Information Commissioner has indicated that consent should be informed and unambiguous, particularly in the case of sensitive personal information. If consent is sought, the individual should understand how their information will be used, and for what purpose.

The gateway and exemption conditions that can be used to allow information sharing are provided in detail in Annex A of the Channel Duty guidance 2020: Sharing information with partners

The data that Panel members may be expected to share about an individual might include (but may not be limited to):

- Demographics (name, date of birth, gender, address, ethnicity)
- Offending history
- Living Arrangements
- Family and personal relationships
- Statutory education
- Neighbourhood
- Lifestyle
- Substance misuse
- Emotional and mental health
- Perceptions of self
- Thinking and behaviour
- Attitudes to engagement in relevant activity
- Motivation to change
- Cultural factors

All member organisations will take steps to ensure that information shared in Channel Panel is not stored or held in their agencies, for example VAF's/ channel minutes – these should be stored as outcome logs.

Appendix 9 - Serious and Organised Crime Joint Action Group (SOCJAG) Confidentiality Declaration Sign-in Sheet

Name of the meeting: Serious and Organised Crime Joint Action Group (SOCJAG)

Date of meeting:

Chair:

Purpose of the meeting:

The Warwickshire Serious & Organised Crime Joint Action Group [SOCJAG] has been set up to allow law enforcement and partner agencies (Partners) to work together to understand the threat around Serious Organised Crime; to share information and good practice and to identify opportunities for joint working, ensuring all available information and powers are used against the organised crime threat. It also seeks to embed the principles of prevent, prepare, protect, and pursue in accordance with the Government's Serious Organised Crime Strategy [2018].

As part of the SOCJAG, Partners will work together to tackle Serious Organised Crime to reduce the impact that this has on the local communities, especially the most vulnerable, businesses and the wider economy.

Any personal information or sensitive personal information known as special category data disclosed to you during this meeting has been provided to you in strict confidence and for the purpose of:

1. The detection of crime and anti-social behaviour
2. The prevention of crime and anti-social behaviour
3. The apprehension of an offender for crime or anti-social behaviour
4. The prosecution of an offender for crime or anti-social behaviour

subject to Section 115 Crime and Disorder Act 1998, the General Data Protection Regulations 2016/679, and Data Protection Act 2018 in particular exemptions to UK GDPR set out at Schedule 2 Part 1 Section 2 Data Protection Act 2018.

All signatories agree that:

- The information shared is done so on a lawful basis. The lawful basis relied upon is to perform a task in the public interest. The lawful basis for processing special category data is in the substantial public interest for the administration of justice. Information should only be shared on a need-to-know basis and must not be disclosed to any third party, including the data subject and other staff who do not have direct involvement in the original purpose for which it was disclosed.

  Further dissemination will only be permitted where there is a lawful basis to do so.

  Where a partner agency requires information for evidential purposes, this cannot be taken directly from meeting discussions and/ or circulated papers. A data protection request (within the Community Safety Information Sharing Protocol - appendices 11 and 12) should be submitted to the data owner to request the specific information in a legally compliant format.

- Data must be stored securely and permanently deleted when it is no longer required for the purpose for which it is provided.

- Any information shared is only valid at the time of provision and should only be used for the purpose as disclosed. It is only disclosed for the specific purpose given at the time of disclosure and should not be used for any other purpose.

- Any information shared will be proportionate and necessary for the purpose for which it is being shared.

- Where possible information shared must be handled and stored in accordance with the Government Security Classifications.

- Where personal information is shared with organisations that do not have access to secure email addresses, it must be encrypted with a password.

- Attendees joining the meeting virtually must ensure that confidentiality is maintained throughout.

- Meetings will not be recorded.

- All persons signing this document are duly authorised to act on behalf of their respective organisation to adhere to the conditions set out.

Please note, by signing this sheet you are agreeing to comply with the requirements of the Safer Warwickshire Partnership Board Community Safety Information Sharing Protocol.

Name	Signature	nisation Represented

Appendix 10 - Warwickshire Domestic Abuse Perpetrator Programme Panels – Information Sharing Statement

W-DAPP operates subject to General Data Protection Regulations (GDPR), the Data Protection Act 2018, Warwickshire Community Safety Information Sharing Protocol & the W-DAPP provider's Information Security & Data Protection Policy and this document.

W-DAPP is provided as a 'with consent' service. It is the responsibility of the referring agency to obtain the valid consent of DA Perpetrators for a referral with their information to be submitted to the W-DAPP provider.

Where the consent of an individual cannot be obtained information should only be shared where a statutory exemption is identified as set out in the Data Protection Act 2018 or where the sharing of information is necessary to prevent death or serious harm.

Information received by the W-DAPP provider will be processed in line with their Information Security & Data Protection Policy.

Where consent has been previously given but subsequently withdrawn, the W-DAPP provider will ensure there is a GDPR compliant process in place for deleting personal data that should no longer be retained.

The owner of W-DAPP records for the purposes of disclosure will be the Partner Agency concerned. W-DAPP is not an agency for the purposes of criminal or civil disclosure requests.

Appendix 11 - Request from external agencies to the Police for information

REQUEST MADE TO WARWICKSHIRE POLICE BY OTHER AGENCIES FOR INFORMATION

DETAILS OF ORGANISATION REQUESTING INFORMATION:	
Name of applicant:	
Address / Organisation:	
Tel:	
Date	

To:	

I AM REQUESTING PERSONAL INFORMATION ABOUT: (The details of the person you are managing)			
Surname:			
Forename(s):			
Also Known as:			
Place of Birth:			
PNC ID:		Date of Birth:	
Full Present Address:		Postcode:	
Previous Address:		Postcode:	

PLEASE ANSWER ALL 5 POINTS BELOW BEFORE SUBMISSION:

1. The offence and circumstances for which the subject is being managed.
2. The time parameters you want the searches over or between, up to a max of 12 months and The reason for the search.
3. Exactly what you want searching, i.e., intelligence / police call outs / arrests / addresses etc. Please do not put all of them in every request unless you are able to show justifications.
4. If you also require information regarding other persons (partners/family/friends), you must provide their full name and dob for us to positively identify them and provide full justifications as to why this information is needed.
5. If your subject is moving to an address, please confirm if this address will be empty or will there be other occupants, if there are others then we would need to have their details to advise.

Note: Local intelligence systems for Warwickshire Police will be checked only, unless specified by the requestor, national checks will include a significant delay.

1	
2	
3	
4	
5	

I HAVE A LEGAL BASIS UNDER GDPR OR DATA PROTECTION ACT 2018 AND THE REASONS ARE:
Intelligence requests are not completed by default. In line with Government GDPR Guidance and the Data Protection Act 2010, if there is an identified and evidenced risk to the public, the nature of the offence committed by a related Service User is identified a risk to the public, and/or if the whereabouts of the identified person indicates an increased risk to the public, a request for intelligence information is made.
Common Law Duty of Confidentiality – I confirm that the duty of confidentiality can be overridden in this situation. Human Rights Act 1998 Article 8: Right to Privacy – The right to privacy of the individual concerned has been considered but the public interest served in disclosing the personal data, outweighs the right to privacy.

Signed:		Rank/Title:	
Name:		Date:	

RESPONSE TO REQUEST

Disclosure of personal data must be relevant, justified and the minimum amount required for the purpose and compatible with the data protection principles.

DETAILS OF WARWICKSHIRE POLICE CONTACT			
Name:	FIB		
Address:	Warwickshire Police		
Tel:	01926 415000	Email:	fib@warwickshire.police.uk
Date:		Our Ref:	

The response to your request is detailed below and has been provided for the sole purpose outlined in your request and therefore this information will not be disclosed to a third party and will not be used for any other purpose.			
Signed:		Rank/Title:	
Name:		Date:	
THIS FORM MUST BE QUALITY ASSURED BY A NAMED POINT OF CONTACT (POC):			
Signed:		Rank/Title:	
Name:		Date:	

All information exchanged will only be so exchanged within the statutory framework of the Information Sharing Agreement and should be obtained, held, retained and disposed of in a fair, lawful, secure and appropriate manner in accordance with the Data Protection Act 2018 and the retention and disposal/destruction policies of Warwickshire Police.

If you receive a subject access application and personal data is identified as belonging to Warwickshire Police, it is your responsibility to contact us to determine whether we wish to claim an exemption under the provisions of the Data Protection Act 2018.

Appendix 12 - Request from the Police to external agencies for information

Request to external organisation for the disclosure of personal data to the police
Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d) & 9(2)(c)

To:	
Position:	
Organisation:	
Address:	

I am making enquiries which are concerned with (mark as appropriate):

The prevention or detection of crime

The prosecution or apprehension of offenders

Protecting the vital interests of a person

I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters.

I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above.

Information required:

Why the information is necessary for the purpose:
Beware of disclosing information which is excessive or may pose operational risks to your investigation, but also be aware that failure to explain the necessity clearly may delay or prevent disclosure.

Police reference:

From:	
Rank/number/name:	
Station:	
Date/time:	
Tel no(s):	
Email:	
Signature:	
Counter signature: **	
Rank/number/name:	

** as required by recipient

Please see Guidance Notes on following page.

Undertaking of lawful use of data disclosed to the police service:

Information disclosed to the police service is protected against unlawful reuse by the second data protection principle*, which prohibits data collected for one purpose being reused for another. If data disclosed to the police service is needed for another purpose, it will be reused only if the new purpose is lawful or a lawful exemption applies, and only data necessary and proportionate to that new purpose will be used.

Therefore, the police service undertakes to ensure that any use or reuse of the data disclosed is lawful, compliant with the data protection principles and processed using appropriate safeguards to the rights and freedoms of the data subject.

Please be aware that we cannot comply with a request to limit use of data which is overridden by a statutory or common law duty or obligation. However, the reuse will be subject to the safeguards described above.

We respectfully request that the same or equivalent measures are observed in your handling of this request for information.

Additional information you may wish to provide to the police service:

In order to help us safeguard against risk to the data subjects, your organisation, and the police service, please provide with your disclosure any additional information you believe necessary to best handle the data you choose to disclose. This may include, but is not limited to:

- Risks we could not reasonably anticipate
- Any expectation to consult with your organisation should reuse be necessary
- Legally enforceable restrictions on reuse of the data

Explanatory Note

This form is used by the police when making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Crime and Taxation - The GDPR regulates the processing of personal data where it is done so for non-Law Enforcement purposes. Article 23 of the GDPR permitted the UK Parliament to create, via legislation, exemptions from particular elements within the GDPR which would otherwise compromise the public interest. The Data Protection Act 2018 sets out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within the GDPR do not apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general). This applies where personal data is disclosed by an organisation subject to the GDPR to the police for the purposes of *the prevention or detection of crime* or *the apprehension or prosecution of offenders*.

It restricts the application of the GDPR data protection principles and subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice *the prevention or detection of crime* or *the apprehension or prosecution of offenders*.

* General Data Protection Regulation Article 5(1)(b) and Data Protection Act 2018 Part 3 Section 36

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or Data Protection Act 2018.

Organisations already processing data for the prevention and detection of crime may wish to consider compatibility with their conditions for processing instead of using this exemption. For example, Schedule 1 Part 2 Paragraph 10 provides the condition for processing (including disclosure) for purposes compatible with this request.

Vital Interests – To protect life or prevent an immediate and credible risk to life, GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure *is necessary in order to protect the vital interests of the data subject or of another natural person.* Article 9(2)(c) provides for processing of special category data to the same ends, where the data subject is legally or physically incapable of consent.

Further guidance on the use of this form may be obtained from your Data Protection Officer.

Completion Guidance

Police officers or staff completing this form should type and tab between the fields on the form. The information required field should provide the recipient with sufficient information to allow them to locate the information sought. Where a signature and/or counter signature are required the form will need to be printed off and signed manually. Some organisations may require a counter signature to be added to the form. Normally this should be the supervisor or line manager of the person completing the form, but may be a higher rank if reasonably required by the recipient.

Investigatory Powers Act 2016

From February 2023 communication data held by a telecommunication operators can no longer be obtained under the Data Protection Act 2018. This data must be obtained via an application under the Investigatory Powers Act 2016. Examples of such data are IP address at point of registration and IP Log on History. If you are unsure please contact the Communication Data Investigation Unit for further guidance.

Appendix 13 - Safer Warwickshire Partnership Board Signatures

Organisation [3]	Chief Officer signatory and role	Designated Officer(s)	Contact details.
Warwickshire County Council	Monica Fogarty- Chief Executive	Tami Battle - EA to the Chief Executive	tamibattle@warwickshire.gov.uk
		Shade Agboola - Director of Public Health	shadeagboola@warwickshire.gov.uk
		David Ayton-Hill - Director of Transport and Economy	davidayton-hill@warwickshire.gov.uk
		John Coleman- Director of Children and Families	johncoleman@warwickshire.gov.uk
		Pete Sidgwick- Director of Social Care and Support	petesidgwick@warwickshire.gov.uk
		Sally Waldron - Assistant Chief Fire Officer	SallyWaldron@warwickshire.gov.uk
		Johnny Kyriacou – Director of Education	johnnykyriacou@warwickshire.gov.uk
North Warwickshire Borough Council	Steve Maxey- Chief Executive	Julie Taylor - Senior Policy Support Officer	SteveMaxey@NorthWarks.gov.uk JulieTaylor@NorthWarks.gov.uk

[3] The Police and Crime Commissioner is also a member of the Safer Warwickshire Partnership Board. He is not included as a signatory as his team are not involved in partnership meetings where the level of personal information covered within the protocol is discussed.

Nuneaton and Bedworth Borough Council	Nicola Botterill – Assistant Director (Social Housing and Community Safety)	Abubaker Malek - Communities and Community Safety Manager	Nicola.Botterill@nuneatonandbedworth.gov.uk Abubaker.malek@nuneatonandbedworth.gov.uk
Rugby Borough Council	David Burrows - Chief Officer Regulation and Safety	David Burrows Paul Pritchett - Environmental Health & Community Safety Manager Supported by Matthew Deaves- Communication Consultation and Information Manager	david.burrows@rugby.gov.uk paul.pritchett@rugby.gov.uk matthew.deaves@rugby.gov.uk
Stratford-on-Avon District Council	Marcia Eccleston – Head of Law and Governance and Monitoring Officer	Phoebe Knowles – Information Governance Officer Sam Slemensek – Community Safety Manager	Marcia.Eccleston@stratford-dc.gov.uk Phoebe.Knowles@stratford-dc.gov.uk Sam.Slemensek@stratford-dc.gov.uk
Warwick District Council	Marianne Rolfe – Head of Safer Communities, Leisure and Environment	Marianne Rolfe Supported by Gerard Grey- Information Governance manager	Marianne.Rolfe@warwickdc.gov.uk
Warwickshire Police	Alex Franklin-Smith – Chief Constable	Sara Smith - Head of Information Assurance & DPO	informationassurance@warwickshire.police.uk
Probation Service	Andy Wade – Head of Service (Warwickshire)	Chloe Davies – Deputy Head of Service (Warwickshire)	Andy.Wade@justice.gov.uk Chloe.Davies@justice.gov.uk

NHS Coventry and Warwickshire Integrated Care Board (ICB)	Jamie Soden – Interim Chief Nurse	Jackie Channel – Associate Chief Nurse	jamie.soden1@nhs.net jackie.channell@nhs.net
Equality and Inclusion Partnership (EQuIP)	Junaid Hussain- Chief Executive	Junaid Hussain	junaid@equipequality.org.uk
Warwickshire Neighbourhood Watch Association	Colin Cartwright - Chair	Colin Cartwright	colincartwright@warwickshirenhw.org.uk

Appendix 14 - Additional Signatures and Designated/ Lead Officers

Organisation	Chief Officer signatory and role	Designated Officer(s)	Contact details
Arnold Lodge School	Matt James - Head of School	Matt James	mjames@arnoldlodge.com
Aylesford School Warwick	Donna-Marie Savage – Director of Safeguarding	Donna-Marie Savage	savage.d@aylesfordschool.org.uk
Barnardo's	Jarvia Blake - Assistant Director – Children's Services	Jarvia Blake	jarvia.blake@barnardos.org.uk
Bradby Club	John Robertson, Club Leader/Safeguarding Lead	John Robertson	john@bradby.org.uk
Bromford Housing	Donna Scott - Community Safety Team Manager	Donna Scott	Donna.Scott@bromford.co.uk
Campion School	Nick Hawkins – Assistant Head Teacher	Nick Hawkins	Nickh1@campion.warwickshire.sch.uk
Canal and River Trust	Henriette Breukelaar – Regional Director West Midlands	Henriette Breukelaar	henriette.breukelaar@canalrivertrust.org.uk
Change, Grow, Live (CGL)	Kirsten Lord - Warwickshire Services Manager	Kirsten Lord	Kirsten.Lord@cgl.org.uk
Citizen Housing	Kevin Rodgers - Chief Executive	Sangita Mundy	reportsafeguarding@citizenhousing.org.uk
COMPASS (Young People's Criminal Justice substance misuse service)	Richard Thomas – Service Manager	Richard Thomas	Richard.Thomas@compass-uk.org

Coventry & Warwickshire NHS Partnership Trust (South Warwickshire Recovery Team)	Suzanne Madle -Williams – Head of Service for Community Mental Health (South Warks)	Suzanne Madle-Williams	Suzanne.Madle-Williams@covwarkpt.nhs.uk
Coventry Cyrenians	Waqas Ali – Operations Lead	Waqas Ali Paul Fitzgibbon	waqas.ali@coventrycyrenians.org paul.fitzgibbon@coventrycyrenians.org
Department for Work and Pensions	Andy Hobbis – Partnership Manager	Andy Hobbis	andy.hobbis@dwp.gov.uk
Doorway	Jenni Muskett - CEO	Laura Summers – Advice Service Manager Lyndsey Stockley – Support Service Manager	laura.summers@doorway.org.uk lyndsey.stockley@doorway.org.uk
Equation	Marie Bower | Head of Service (Survivors and Perpetrators)	Marie Bower	marie@equation.org.uk
Family Intervention Counselling Service	Donna Hodge - Director and Trainee Forensic Psychologist	Donna Hodge	admin@interventionservice.co.uk
Futures Unlocked	John Powell - Operations Manager	John Powell	admin@futuresunlocked.org John.powell@futuresunlocked.org
Get-to CIC	Lloyd Robinson- Managing Director	Lloyd Robinson	l.robinson@get-to.co.uk
HCRG Care Group Ltd	Sarah Wardle - Chief Nursing Officer, DIPC, Caldicott Guardian	Aneesa Jamil - Named Nurse-Safeguarding Children	aneesa.jamil@hcrgcaregroup.com
Helping Hands Community Project	Jo Merrick – Client Service Manager	Jo Merrick	jo@helpinghandscharity.org.uk

HMP Featherstone	Warren Sullivan - Governor	Rachael Lindop	rachael.lindop@justice.gov.uk
Listening Ear	Michelle Lyons - CEO	Tracey Allen-Lea (Head of Clinical Services)	Tracy.Allen-Lea@listening-ear.co.uk
Mediation and Community Support service	Judith Halliday - Conflict Resolution Worker and Trainer	Judith Halliday	admin@mediationsupport.org.uk
Midland Heart (Housing Association)	Rebecca Larkin – Head of Tenancy and Safer Neighbourhoods	Sue Lamb	Rebecca.Larkin@midlandheart.org.uk sue.lamb@midlandheart.org.uk
My Local Bobby Ltd	Ahmet Izzet - COO	Luke Gilding – Regional Manager	luke@mylocalbobby.co.uk
Myspace Housing	Rachael Reeves - Housing Manager (Midlands)	Rachael Reeves	rachael.reeves@myspacehousing.org
Myton School	Neil Phipps – Deputy Head Teacher	Neil Phipps	phipps.n@myton.co.uk
New Meaning Training	Alex Cooper - Area Manager	Alex Cooper	alex.cooper@newmeaning.training
North Leamington School	Simon Owen – Deputy Safeguarding Lead	Simon Owen	sowen@northleamington.co.uk
Orbit Group	Andrew Meyer - Head of Tenancy Services	Andrew Meyer	andrew.meyer@orbit.org.uk
Platform Housing Group	Catherine Cole – Assistant Director	Jon Elger	info@platformhg.com
P3 Social Inclusion Charity	Esther Barrett – Head of Support and Community Services	Henry Webster	info@p3charity.org

Refuge	Denise Brown – Director of Service Delivery	Melanie Jones – Service Manager Lottie Mayers MARAC Coordinator	Melanie_Jones@refuge.org.uk Lottie_mayers@refuge.org.uk
RoSA (rape or sexual abuse support)	Julie Bettelley - CEO	Julie Bettelley	julie.bettelley@rosasupport.org
Rugby First	Luke Phillips – Control Room Manager/BID Manager	Luke Phillips	luke@rugbyfirst.org
Safeline	Neil Henderson - CEO	Neil Henderson	neil@safeline.org.uk
Sage Homes	Amanda Mitchell -Partnerships Administrator	Amanda Mitchell - Partnerships Administrator	residentservices@sagehomes.co.uk
Salvation Army – Leamington Spa Church	Sarah Johnson – Salvation Army Officer, Church Leader	Sarah Johnson	Leamington.Spa@salvationarmy.org.uk
South Warwickshire University NHS Foundation Trust	Charles Ashton – Medical Director	Charles Ashton	charles.ashton@swft.nhs.uk
Southern Housing	Louise Thomas – Head of Region	Marcus Crockett	Marcus.crockett@southernhousing.org.uk
Spring Housing	Raj Shergill - Director of Housing & Customer Services	Raj Shergill	rajbir@springhousing.org.uk
St Giles Trust	Steve Clarke – Regional Delivery Manager	Hannah Whiteley – Community Delivery Manager	Hannah.whiteley@stgilestrust.org.uk
Stepping Stones Stratford on Avon	Richard Heathcote - Trustee	Mandy Scruby - Manager	mgr@steppingstonessoa.org
Stonewater	Catherine Preece – Area Manager	Catherine Preece	catherine.preece@stonewater.org

Stratford-upon-Avon Street Pastors	Maureen Lynda Green - Coordinator	Maureen Lynda Green	stratforduponavon@streetpastors.org.uk
Stratford BID Ltd	Aaron Corsi – BID Manager	Aaron Corsi	admin@stratforduponavonbid.co.uk
Victim Support Warwickshire	Deborah Miller - Senior Operations Manager	Deborah Miller	deborah.miller@victimsupport.org.uk
Walsall Housing Group	Suzanne Gill - Data Privacy Manager and DPO	Suzanne Gill	Suzanne.Gill@whgrp.co.uk
Warwickshire Counselling Centre	Julie Mitchelson – Assistant Manager (Children & Young People) / Administrator	Julie Mitchelson	julie.mitchelson@sycamorecounselling.org.uk
Warwickshire Retail Crime Initiative	Derek Bradley, P.J. Seal (WRCI Administrators) Peter Guillaume (Volunteer Manager)	Derek Bradley P. J. Seal Peter Guillaume	wrcinorth@wrci.org.uk wrcisouth@wrci.org.uk admin@wrci.org.uk
Warwickshire Rural Housing Association	Philippa Osborne - Area Housing Manager	Philippa Osborne	philippa.osborne@midlandsrural.org.uk
Warwickshire Search and Rescue	Ian Malins – Chair	Ian Malins	chair@warksar.org.uk
West Midlands Anti-Slavery Network	Nigel Oseman -Independent Modern Slavery Advocate	Nigel Oseman	nigel.oseman@westmidlandsantislavery.org
Young People First	Jo Squires – CEO	Jayne Thomas – Outreach Manager	jayne.thomas@youngpeoplefirst.org.uk
Youth Escape Arts Escapearts.org	Anthony Bishop – Operations Manager	Sarah Cowley-Catchpole	Sarah@stratfordyouth.org