Information Sharing Agreement

West Midlands Police
and
Multi-Agency Referral Assessment Conferences (MARAC)

Contents

1 Introduction

This Information Sharing Agreement (ISA) has been created at the request of the Information Security & Assurance Team - West Midlands Police, and MARAC & Partner agencies involved.

Current arrangements are in place for the sharing of information between agencies who attend the Multi-Agency Referral Assessment Conference meetings across the West Midlands Police Force area and West Midlands Police. This agreement seeks to clarify the detail of these arrangements.

All MARACS & Partner agencies will agree with terms laid out in this main Information Sharing Agreement.

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

2 Purpose

The purpose of this document is to set out the terms and conditions under which data held by West Midlands Police and MARAC agencies will be shared. This framework recognises that effective joint working is vital in the prevention of crime, protecting the public, and helping those in need.

MARAC is a multi-agency meeting focusing on the safety of victims of domestic violence/abuse assessed as high risk of serious harm or homicide. The aims of the MARAC are to:

- Share information to increase the safety, health and wellbeing of the domestic violence/abuse victims at high risk of serious harm or homicide and their children;
- Determine whether the perpetrator poses a significant risk to any individual or to the general community;
- Jointly construct and implement a risk management plan that provides professional support to all those at risk that reduces the risk of serious harm.
- Track actions and where necessary, follow up at the next meeting.
- Reduce repeat victimisation.
- Improve agency accountability
- Improve support for staff involved in high risk domestic violence/abuse cases by sharing the burden of risk.

MARAC is predicated on the need to share only accurate information that is directly relevant to the safety of victims.

Information is shared by West Midlands Police under the Crime and Disorder Act 1998, and is shared for law enforcement processes under s.31 of the Data Protection Act 2018, namely for the purposes of prevention and detection of crime (serious harm or death). Partner agencies which are public bodies share information as necessary for the performance of tasks carried out in the public interest, or in the exercise of their official authority. Voluntary sector partner agencies share information on the grounds of their legitimate interests as organisations with a safeguarding mandate.

All partner agencies will maintain and follow their own internal policies for information sharing, which will specify how information sharing within MARAC is consistent with the

purpose for which the information was originally gathered. Information will be shared in line with Caldicott Principles.

Information shared falls into four main categories:

- Demographic information including victims' and perpetrators' names, dates of birth, addresses, ethnicity and any pseudonyms used and the names and dates of birth of any children. (The MARAC referral form can be found at Appendix 2 of the West Midlands MARAC Operating Protocol)
- Information on key risk indicators including where appropriate, professional opinion on the risk faced.
- Relevant history of domestic violence/abuse or associated issues (child abuse, sexual assault) for the perpetrator or victim.
- Views of the victim.

The role of MARAC is to facilitate, monitor and evaluate effective information sharing that enables appropriate actions to be taken to increase public safety. The responsibility to take appropriate action rests with individual agencies; the responsibility is not transferred to MARAC.

The benefits of information sharing to all partners include:

- To help risk assessment and decision making between the partners to be as fully informed as possible, by enabling a full picture to be gained of the background and events leading up to incidents of domestic violence and their resultant harm and for underlying reasons to be understood
- To support decision-making with regard to whether cases should be referred to the Multi Agency Risk Assessment Conference (MARAC) process
- To better inform decision-making with regard to whether there is any ongoing risk of exposure of individuals (including children) to domestic violence
- To support decision-making about actions which may be appropriate with regard to alleged offenders to inform partners of case outcomes, enabling lessons to be learned
- To support the review of previous decisions taken by the partners and decision-making procedures, where opportunities are identified to tackle problems in other ways, or to 'do things differently next time'
- Helping WMDVP staff and personnel to make properly informed and balanced decisions in relation to their own safety, by alerting them to any known potential risks which may arise during their contact with people involved in domestic violence incidents and especially where the information may not be available from any other source.

All referring agencies should discuss consent and explain the MARAC process to the victim. Where consent from the victim is not obtained, the case should still be referred with the reason recorded on the MARAC referral form, in accordance with individual organisation's information sharing policies and protocols. Consent is not required for referral to MARAC, so long as the test of 'high risk of serious harm or homicide' is met.

This purpose is consistent with West Midlands Police's obligations under the Data Protection Act 2018, with reference to the General Data Protection Regulations (EU 2016/679) and

The Law Enforcement Directive (EU/2016/680), effective from May 2018, including being consistent with the original purpose of the data creation / collection.

3 Powers and Legal Framework

The principal legislative instruments that should be considered when sharing information under this agreement are:

- The Crime and Disorder Act (1998) (requirement on responsible bodies – including policing bodies and local authorities - to formulate and implement crime and disorder strategies)
- The Data Protection Act (2018) (legislation in support of the GDPR which provides supplementary definitions, and gives effect to the Law Enforcement Directive by applying a version of GDPR to law enforcement processing)
- EU Regulation 2016/679 – The General Data Protection Regulation (European legislation having direct effect in the UK which lays down rules for the protection of the processing of personal data of natural persons. Does not apply to processing for law enforcement purposes)
- EU Directive 2016/680 - The Law Enforcement Directive (European directive that EU Member States – including the UK – introduce rules which protect the processing of personal data for the purposes of prevention, investigation, detection nor prosecution of criminal offences or the execution of criminal penalties)
- The Freedom of Information Act (2000) (creates a public 'right of access' to information held by public authorities)
- Human Rights Act (1998) (incorporates the major rights from the European Convention on Human Rights into domestic British law. These include the A3 right to life and A8 right to respect for private and family life, which are both relevant to information sharing with MARAC)
- The Rehabilitation of Offenders Act (1974) (sets out rehabilitation periods for particular sentences, and limits disclosure of previous convictions)
- The Children's Acts of 1989 and 2004 (allocate duties to safeguard children and their welfare)
- The Care Act 2014 (includes protection for safeguarding adults at risk of abuse or neglect)
- Common Law Powers of disclosure (various, including the power to disclose confidential information without consent if there is an overriding interest in favour of disclosure)

There are other pieces of legislation that place powers or duties to share information on public authorities – this list is not meant to be exhaustive. All information sharing must be conducted in accordance with one or more of the legal powers / duties.

3.1 Data Protection Principles within GDPR

The data protection principles which set out the main responsibilities for how data should be processed are defined in Article 5 of the GDPR (for organisations) and Sections 35 to 40 of the Data Protection Act 2018 (for law enforcement processing):

#	Principle Description	Evidence/Rationale
1st principle	a) Processed lawfully, fairly *and in a transparent manner in relation to individuals*;	Lawful processing may be: (for public bodies) the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law (for voluntary sector) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (for law enforcement purposes by police) the processing is necessary for the performance of a task carried out for that purpose by a competent authority Special rules apply to the processing 'special category' data and data concerning criminal convictions and offences. Transparent processing is not required for law enforcement processing by police. It is required for other partner agencies, which means that appropriate privacy notices under A13 and A14 GDPR must be provided. It is the responsibility of individual partner agencies and data controllers to supply those notices.
2nd principle	b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;	The data is to be collected and shared to: - Increase the safety, health and wellbeing of the DA victims at high risk of serious harm or homicide and their children. - Determine whether the perpetrator poses a significant risk to any individual or to the general community. - Jointly construct and implement a risk management plan that provides professional support to all those at risk that reduces the risk of serious harm. - Track actions and where necessary follow up at the next meeting - Reduce repeat victimisation - Improve agency accountability - Improve support for staff involved in high risk DA cases by sharing the burden of risk The data will only be shared with the named partners of this ISA who will not share it with any unnamed or unauthorised persons or organisations without prior consultation and expressed authority from the data controller.

#	Principle Description	Evidence/Rationale
3rd principle	c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	Only relevant data will be shared. It is the responsibility of the data controller (i.e. each individual partner agency) to make sure that the information shared is adequate, relevant and limited to what is necessary for the purpose of the MARAC. The MARAC Chair will monitor sharing during the meeting and limit inappropriate sharing. For further details please see section 5
4th principle	d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	Data controllers are responsible for ensuring that the information they bring to MARAC is accurate, and where relevant that it is kept up to date. When MARAC conferences occur any information that is shared with partners will be validated in the meeting wherever possible and WMP MARAC systems updated to reflect any changes. Incorrect data will be amended before further MARAC information is shared with partners.
5th principle	e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;[1]	WMP will keep records of all MARAC referrals and cases using a Share Point system. Cases where there is no activity for 12 months will be flagged on the system and, where necessary (if there is no ongoing case) archived and logged as a "closed case" on Share Point. Cases will be kept indefinitely for the purposes of risk management. The information shared at MARAC meetings by WMP is by verbal update. Any paper documentation is shredded after the meeting. An electronic version of the information is shared by the MARAC Admin and Coordinator via a 7 Zip encrypted email. Information received by partner agencies will be reviewed in accordance with each organisations own internal policies and procedures and kept for as long as they are needed in accordance with those procedures.

[1] personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

#	Principle Description	Evidence/Rationale
6th principle	f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	The data will only be shared with agencies signed up to the MARAC Operating Protocol and this Information Sharing Agreement. The MARAC Agencies agree to apply appropriate security measures commensurate with the requirements of principle 6 of the Data Protection Act (2018), and principle 6 (Sec. 89) of the General Data Protection Regulation (EU 2016/679). In particular, they will ensure that measures are in place to do everything reasonable to mitigate against risks including accidental or unauthorised access, destruction or loss, use, modification, or disclosure of personal data. The MARAC Agencies will ensure that appropriate security measures shall be applied at all times. Whilst certification to ISO/IEC 27001:2013 may not be possible for some partners, all signatories should seek to comply with the principles contained in the ISO/IEC 27000 series. Data to be protected by digital encryption where available. Emailing from WMP to agencies and MARACS need to be encrypted (7ZIP). The WMP Share Point system which contains records of all MARAC referrals and cases will be subject to access controls, such that access is restricted to those with genuine 'need to know' within WMP.

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

3.2 Special Category Data within GDPR / Sensitive processing in Data Protection Act 2018

Special category data is defined as more sensitive within GDPR, and so needs more protection. For example, information about an individual's:

- Race or Ethnic Origin
- Political opinions
- Religious or philosophical beliefs
- Trades union membership
- Genetic data
- Biometrics (where used for the purposes of identifying a natural person)
- Health
- Sex life
- Sexual orientation

Law Enforcement processing (governed by DPA 2018): Competent Authorities must have a lawful basis for processing sensitive data, as defined in section 35 of the DPA 2018.

Processing by other partner agencies (governed by GDPR) In order to lawfully process special category data under GDPR, partner agencies must identify both a lawful basis under Article 6 (See Appendix A of this document) and separate conditions for processing special category data under Article 9(2) (see Appendix B), and criminal conviction data under Article 10.

The special conditions in Article 9(2) which allow processing of special category personal data include:

- Article 9(2)(b) – for employment, social security and social protection purposes
- Article 9(2)(g) – for substantial public interest purposes
- Article 9(2)(i) – for public health purposes
- Article 9(2)(j) – for archiving, research and statistics purposes

Article 10 GDPR requires that the processing of criminal convictions data is prohibited unless it is carried out under the control of official authority or if it is authorised by UK law. Member States may authorise the processing of criminal convictions personal data in specific circumstances and subject to appropriate safeguards.

It is for each partner agency to satisfy itself that it holds lawful grounds for processing special category data and data relating to criminal convictions and offences. It is relevant to observe that the substantial public interest purpose (Article 9(2)(g)) is defined in the Data Protection Act 2018 Schedule 1 Part 2, which includes:

Paragraph 10 (Preventing or detecting unlawful acts) – processing is necessary for the purposes of the prevention or detection of an unlawful act, and must be carried out without the consent of the data subject so as not to prejudice those purposes.

Paragraph 18 (Safeguarding children and adults at risk) – processing is necessary to protect an individual from neglect or physical, mental or emotional harm, or protect their well-being, where they are a child (under 18), or an adult at risk, and consent cannot be obtained because either it cannot be given, or the data controller cannot reasonably be expected to obtain their consent, or where obtaining their consent would prejudice the protection from harm. 'At risk' means that the data controller has reasonable cause to suspect that the adult has needs for care and support, is experiencing – or at risk of – neglect or physical, mental or emotional harm, and as a result of the care / support needs is unable to protect themselves against the neglect or harm or the risk of it.

Policies must be in place to support the processing of sensitive data on both the above grounds, although if a disclosure is made under paragraph 10 to a competent authority then the policy document is not required. West Midlands Police is such a competent authority.

4 The Agreement

This ISA applies to any personal or confidential information, irrespective of the medium in which it is held e.g. paper based, electronic, images. Legal advice on this agreement should be sought in any case of doubt. It should be applied while following established and agreed processes within the signatory organisations.

Under no circumstances should information shared by MARAC partners be retained by the partner agency for longer than is necessary to achieve the purpose specified in this agreement. To gain an exemption to this, a specific request must be sent to the original data controller, who then, following a review, determine if the information can be retained. Files containing information from partner sources will be reviewed in line with force policy.

This agreement does not give agencies an automatic right to receive information or a mandate to provide information, but is a process for information sharing in cases in where it is suitable to do so. By signing up to this agreement, signatories are committed to a positive approach to information sharing, and agree to meet the outlined commitments and processes.

It is the responsibility of each signatory to ensure that:

- Information shared is in accordance with the law
- Appropriate staff training and awareness sessions are provided in relation to this agreement, and that their organisation abides by this document
- Information is shared responsibly and in accordance with professional and ethical standards
- All information is shared, received, stored, and disposed of securely
- Users consider adding the Government Security Classification to documents being shared with partners, including relevant handling instructions where appropriate
- Users adhere to baseline controls for handling police information (Appendix E) in addition to any stipulated handling instructions
- Any restrictions on the sharing of the information contained in the disclosure, in addition to those contained within this agreement, should be clearly noted
- Information exchanges and refusals are recorded in such a way as to provide an auditable record
- Any electronic information exchange is fully secure to UK Government standards (e.g. those email addresses with .pnn, .cjsm, .gsi, .gsx, .nhs, .gcsx, or .mod extensions, or through the use of encrypted and password-protected attachments, the password to be transmitted via phone or text, not email).
- Arrangements are in place to check that this agreement, its associated working practices, and legal requirements are being adhered to
- Any data will only be used for the specific purpose for which it is shared, and recipients will not release information to any third party without obtaining the express written authority of the disclosing partner, including requests from the public
- Arrangements are in place for data subjects to exercise (as available) their rights of information, access, rectification, erasure, restriction, portability, objection, information about automated decision-making and profiling.

5 Data-sharing Protocol

5.1 Specific Procedures

The information that will be shared includes;

- DASH Score
- Date of Referral
- Referral Agency
- Name of Referrer
- Position / Job Title
- Referrer Contact Number
- Victim awareness and consent of the referral
- Reason for non-consent
- Victim details including; Name of Victim, Contact Number (and safe contact number of another person where available), Date of Birth, Gender, Home Address, Current Address, Language Spoken, Ethnicity, Disability, LGBT Relationship Status, GP Surgery, any additional needs, including mental health issues
- Perpetrator details including; Name, Date of Birth, Relationship to Victim, Gender, Usual Home Address, Ethnicity, Current Address, Disability
- Child details including; Name, Date of Birth, Relationship to Victim / Perpetrator, Living with
- Grounds for referral details; Most Recent Incidents, Brief History of Relationship between Victim and Perpetrator, Details of Support and Safeguarding in place, Details of Support and Safeguarding from MARAC if incident has been reported to Police
- Risks and Triggers: to Victim, Children and Offender Triggers
- Police involvement details; Police Crime Reference Number, Safeguarding Officer, Current Offence, SIG Marker (relevant), Non-Molestation or Restraining Order details, Current Offender Disposal status, Bail Conditions, PNC Markers (relevant), Domestic Abuse Offender Management involvement, Charges, Court Data, Sentencing Summary, Safeguarding Summary

All information shared will be relevant and proportionate.

This information will be shared between the MARAC attendees (as required) and between the MARAC Coordinator and Administrator. It will be shared with all MARAC partners after the meeting, by means of distribution of minutes.

The information will be shared both through a single referral form, in person on the agenda, and on papers where necessary. All data that is shared via email will be in an encrypted format, using 7Zip as a level of protection for electronic data transfer.

All agencies who are using paper based copies of MARAC information will ensure that it is securely transported to and from MARAC meetings and destroyed appropriately via the use of a shredder. The retention period for paper copies of MARAC minutes is 12 months.

Paper documents may still be use in some instances should the Share Point system go down, if this happens then once the information is entered into Share Point, any copies should be destroyed post-meeting.

5.2 Further sharing of information

Information about MARAC referrals and cases held on the WMP Share Point system may be further shared for purposes consistent with the purposes set out in Section 2 of this Agreement. Data may be shared with the following bodies:

- Crown Prosecution Service as part of pre-charge or pre-trial disclosure
- Multi-agency panels appointed by Local Safeguarding Children Boards to carry out Serious Case Reviews
- Multi-agency panel caring out a Domestic Homicide Review
- Child Protection Conferences
- Safeguarding Adult Board carrying out a Safeguarding Adult Review

This list is not exhaustive.

All requests from such bodies must go through the West Midlands Police MARAC coordination team, who will redact irrelevant information before any disclosure is made. Where appropriate, public interest immunity will be claimed.

6 Security

The MARAC Agencies agree to apply appropriate security measures commensurate with the requirements of principle 6 of the Data Protection Act (2018), and principle 6 (Sec. 89) of the General Data Protection Regulation (EU 2016/679). In particular, they will ensure that measures are in place to do everything reasonable to mitigate against risks including accidental or unauthorised access, destruction or loss, use, modification, or disclosure of personal data.

The MARAC Agencies will ensure that appropriate security measures shall be applied at all times. Whilst certification to ISO/IEC 27001:2013 may not be possible for some partners, all signatories should seek to comply with the principles contained in the ISO/IEC 27000 series.

Appendix E details the Minimum Protective Measures which must be in place under the Government's General Security Classification for OFFICIAL and OFFICIAL-SENSITIVE categories. Partners should ensure they have appropriate security arrangements in place.

7 Liability

West Midlands Police cannot be held responsible for breaches of this protocol by other MARAC partners or complaints arising from these breaches. MARAC partners are not responsible for breaches of this protocol by West Midlands Police, or complaints arising from these breaches.

Requests for data could be made under the likes of the Data Protection Act or the Freedom of Information Act; such requests can be received by any partner to this agreement (where

relevant). Data that has been shared by a named partner within this agreement with another partner who are considering the release of said data, should first seek advice from the originating partner (prior to release), for instance in the case of West Midlands Police this will help ensure that any data being released will not to prejudice any current investigation(s).

For further details please see relevant partner Privacy Statements. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants, or agents.

It is the responsibility of the partner to ensure it is compliant with this agreement and any associated legislation. It is understood that breaches of this agreement could lead to the termination of this agreement, and in the worst cases, removal of MARAC partnership.

Complaints and breaches must be dealt with by any partner agency in accordance with their policies and procedures.

Data breaches and any immediate action taken to mitigate the risk caused by that breach must also be notified to West Midlands Police without delay, and in any case, within 72 hours.

8 Management and Operation of the Protocol

This ISA will be active from 1st April 2019. For each Local Authority area, the Head of the Community Safety Partnership (or equivalent) will sign this ISA on behalf of all local MARAC partners as defined by the MARAC terms of reference for that area. It shall be the responsibilities of the signatories to ensure that all local partners are aware of their obligations under this Agreement.

The review of this protocol will be completed 6-months after commencement, and annually from the date of commencement thereafter. This will be undertaken by all MARAC partners and coordinated by West Midlands Police MARAC coordination team. The purpose of the review is to ensure it is fit for purpose, covers all that is required and is neither too extensive nor too narrow for its purpose.

Signatories to this agreement shall provide assurance/evidence on request of West Midlands Police Information Management and Information Security Teams to ensure compliance with the information management, security requirements and other obligations detailed in this agreement. Signatories shall provide all reasonable assistance to fulfil this request. The signatory can exercise their rights under this agreement to ask West Midlands Police for evidence of their compliance in relation to its own information shared with West Midlands Police.

Any signatory or partner may request a copy of a signatory / partner's information security policy (where it exists).

Failure to supply sufficient guarantees in respect of security arrangements, or to comply with monitoring processes is likely to result in the termination of the agreement.

9 Signatures

All agencies that are part of the information sharing process will be, upon signing this agreement, bound to comply with its terms.

Within West Midlands Police, the signatory is signing on behalf of the Chief Constable of West Midlands Police.

Signed on behalf of West Midlands Police:

Signatory Name	Signatory Agency	Date Signed	Signature

Signed on behalf of the MARAC Agencies:

Signatory Name	Signatory Agency	Date Signed	Signature

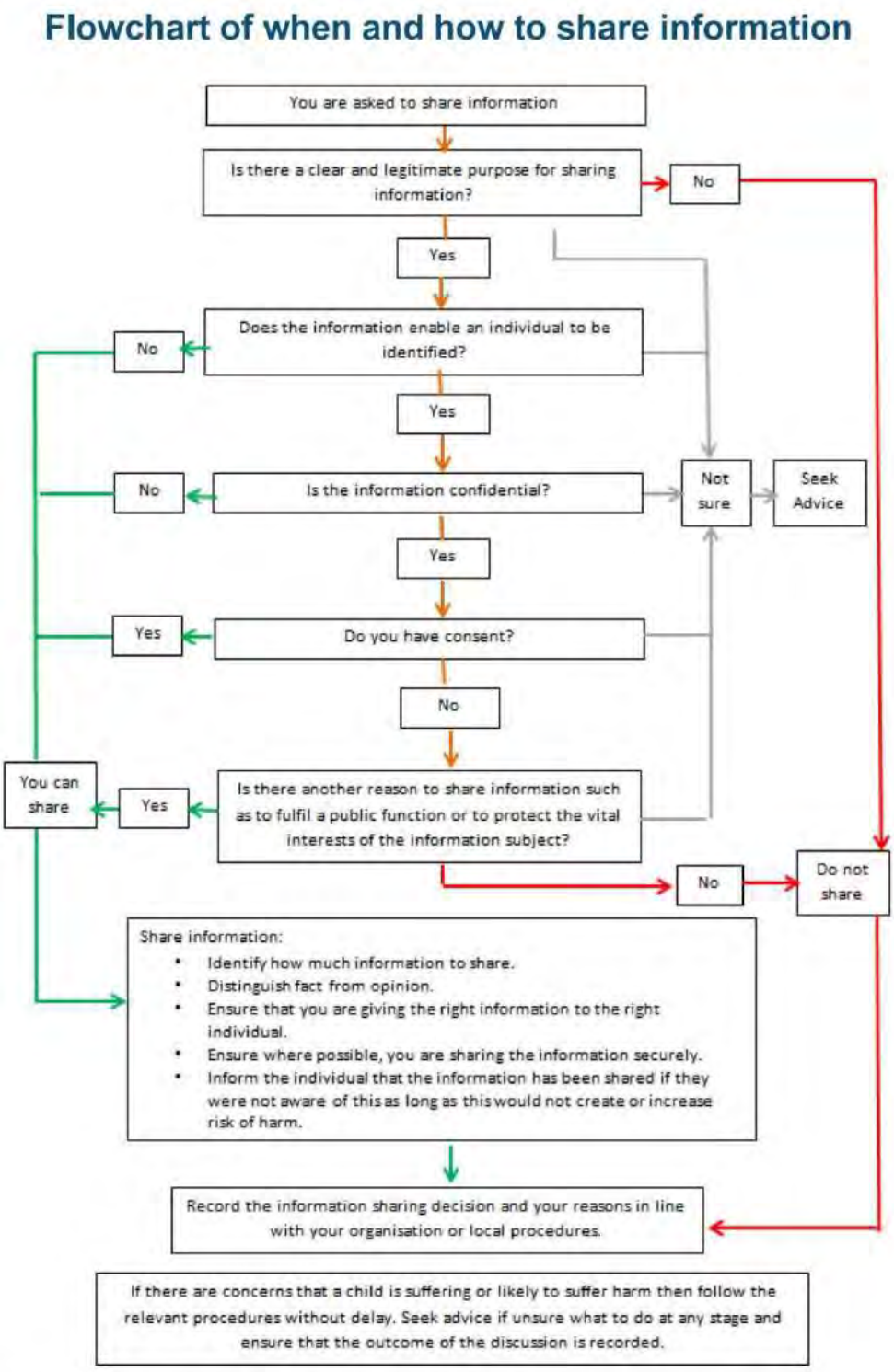
Appendix A: The Lawful Bases for processing Personal Data within GDPR

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix B: The Conditions for processing Special Category Data within GDPR

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Appendix C: Flowchart of When and How to share



Source: Information Sharing (HM Government March 2015)

Appendix D: Definitions

Anti-social behaviour

Anti-social behaviour is defined as acting in a manner, which causes or is likely to cause harassment, alarm, or distress to one or more persons who are not of the same household.

Confidential information

Confidential information is covered by the common law duty of confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

Consent

Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Crime

A crime is defined as any act, default, or conduct prejudicial to the community the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

Data in the public domain

This type of information incorporates any information, which is publicly available, whether it relates to an individual or not.

De-personalised and aggregated information

Where de-personalised or aggregated information is no longer sensitive or identifiable it may be shared outside of the scope of this agreement. However, where de-personalised or aggregated information may still be deemed sensitive (e.g. as a result of complexity, currency, potential for misinterpretation or misuse) it must still be treated with care under the provisions of the ISA.

Disorder

Disorder is considered to be the level or pattern of anti-social behaviour within a particular area.

Information about someone who has died

The GDPR and Data Protection Act 2018 do not apply to information about people who have died. However, such information may still be sensitive, confidential or relate to individuals who are still alive. Information about people who have died must still be shared under the provisions of the ISA.

Information sharing

Information Sharing involves an exchange of information between one or more individuals or agencies.

Personal data

Personal data is defined under GDPR as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Processing of Personal Data

Defined in GDPR in relation to personal data means an operation or set of operations which is performed on personal data or sets of personal data such as;-

a) Collection, recording, organisation, structuring, or storage,

b) Adaptation or alteration

c) Retrieval, consultation or use

d) Disclosure by transmission, dissemination, or otherwise making available

e) Alignment or combination

f) Restriction, erasure or destruction

Special Category personal data (GDPR) / Sensitive data (Data Protection Act 2018)

This is defined as any 'personal data' relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; membership of a trade union; genetic or biometric data (where processed for the purpose of uniquely identifying an individual), data concerning health; sexual life or sexual orientation.

Appendix E: General Security Classification Handling Instructions

	OFFICIAL	OFFICIAL – SENSITIVE
General Points	Be stored and managed securely within Police approved systems Not be accessed, read or discussed where you can be overlooked or overheard Information should be protected by a governance suite including clear desk / clear screen and access control procedures Information may be removed from Force premises provided appropriate safeguards are in place to prevent material being lost or stolen and that authorisation is obtained if significant volumes of material are to be moved You must follow handling instructions from the sender / author	As OFFICIAL, and also: Not be left unattended and should be locked away when not in use Only communicated or passed to others on a need to know basis Information should not be read or worked on in sight of unauthorised persons and that appropriate safeguards are in place to prevent material being lost or stolen
Physical Storage	At least one barrier for physical storage should be used e.g. access cards, locked cabinet Laptops must be locked away or secured in docking stations when left in the office, only encrypted laptops may be taken outside of a Police establishment	
Electronic storage	Any electronic document received marked OFFICIAL should be saved with OFFICIAL in the title and also in electronic document and records management system metadata or notes fields Appropriate controls should be used to limit access Electronic data should be protected when at rest by a combination of physical security and encryption	Any electronic document received marked OFFICIAL-SENSITIVE should be saved with OFFICIAL-SENSITIVE in the title and also in electronic document and records management system metadata or notes fields Appropriate controls must be used to limit both visibility of the document and access to it
Removable Media	Use of removable media should be reduced to the minimum level required to support the business Encryption should always be considered, and where required, should be government-grade	As OFFICIAL, and also: Government-grade encryption should always be used

	OFFICIAL	OFFICIAL – SENSITIVE
Emailing	Information may be sent by secure email (i.e. those containing. pnn, .gcsx, .cjsm, .nhs, .gsi, etc.) Information may be sent to a non-secure email address when appropriate, but steps should be taken to ensure recipients understand any restrictions on further circulation Sensitive or personal data should not be sent without encryption and / or the consent of the person who is the subject of the data	As OFFICIAL, and also: Information may be sent to non-secure email addresses only on an exceptional basis if there is a pressing business need and no viable alternative, provided this is authorised and there is confidence that the recipient will follow any instructions on what can and can't be done with the information
Transporting information (hand / post)	Information may be sent by normal post in a single, unused envelope Sensitive personal data must be double enveloped and either sent by courier / recorded delivery, or on encrypted removable media Seek permission from the Information Asset Owner for significant volumes of information	As OFFICIAL, and also: Include return address on back of the envelope Never mark the classification on the outer envelope, but do mark it on an inner envelope Trusted hand under single cover for physical movement
Telephone	Telephones are inherently insecure, but can be used for conversations classified as OFFICIAL if care is taken to avoid being overheard Sensitive information should not be discussed by telephone, except where the operational value of having the discussion outweighs the risk	
Fax	Always consider using email as a more secure alternative Faxes are inherently insecure, but can be used for material classified as OFFICIAL if the number is confirmed and the recipient is waiting to receive the fax Sensitive information should not be sent by fax, except where the operational value of transmitting the data outweighs the risk	
Printing / Photocopying	Permitted unless handling instructions dictate otherwise Only ever print what you need Control copies appropriately	
Disposal	Information already in the public domain can be disposed of in recycling or general waste Information should be disposed of securely according to internal policy and procedure	