Devon & Cornwall Police

DOMESTIC ABUSE AND SEXUAL VIOLENCE (DASV) INFORMATION SHARING AGREEMENT (ISA)

AGREEMENT FOR THE SHARING OF INFORMATION ON INCIDENTS OF DOMESTIC ABUSE, SEXUAL ASSAULTS AND SEXUAL VIOLENCE IN DEVON AND CORNWALL BETWEEN STATUTORY AUTHORITIES, HOUSING PROVIDERS, VOLUNTARY AND CHARITABLE AGENCIES.

August 2020

Corporate Version 0.6

Owner: Devon and Cornwall Police

Contents

Appendices

Purpose

1.1. The aims and purposes of information sharing within the parties to this Agreement are to:

- identify the true level of domestic abuse and sexual assaults within the Devon and Cornwall areas;
- reduce the incidence of domestic abuse and sexual assaults within the Devon and Cornwall areas;
- encourage the maximum numbers of victims of domestic abuse, sexual assaults and repeat victims to be guided by the recording agency into subsequent multi-agency assistance and support;
- allow those providing the assistance and support to the victim(s) to have all information relating to the pattern of abuse that is required to contribute to an effective outcome;
- allow the assistance providers to feedback details of those entering into assistance to the partnership, in order that reoffending can be identified.

1.2. This Agreement is concerned with the exchange of personal data. Such information may, in certain circumstances, act as a catalyst for an arrest or assist in the correct actions being taken following an arrest when an individual is taken into custody.

2. Powers

2.1. Appendix 1 – Legal Issues identifies the lawful basis for processing.

3. Introduction

3.1. The following organisations, by signing the Certification – Agreement for the Exchange of Information, are deemed to be partners to this Agreement:

Devon & Cornwall Police
Action For Children
Adult Social Care (Cornwall)
Adult Social Care (Devon)
Adult Social Care (Plymouth)
Ahimsa
Army Welfare Service
Aster Group
Babcock LDP
CLEAR
Coastline Housing
Cornerstone Housing Association
Cornwall Council
Cornwall Partnership NHS Foundation Trust
Cornwall Refuge Trust
Ocean Housing
Plymouth and Devon Racial Equality Council
Plymouth City Council
Plymouth Community Homes
Plymouth Community Safety Partnership
Plymouth Domestic Abuse Service (PDAS)
Refuge4Pets
Royal Cornwall Hospitals NHS Trust
Royal Devon & Exeter NHS Foundation Trust
Royal Military Police
Royal Navy Family and People Support (RN FPS)
Salvation Army Housing Association (SAHA)

Devon & Cornwall SARC (Sexual Assault Referral Centre)
Devon County Council
Devon County Council Children's Services
Devon Partnership NHS Trust
Dorset, Devon and Cornwall Community Rehabilitation Companies (CRC)
East Devon District Council
Exeter City Council
Exmouth Children's Centre
First Light Southwest Ltd.
Guinness Trust Housing
Hamoaze House
Harbour Drugs and Alcohol Services
Harbour Housing
Home Group
Livewell Southwest CIC
LiveWest
Mid Devon District Council
NHS Kernow
North Devon Against Domestic Abuse
North Devon District Council
North Devon Homes
Sanctuary Housing
South Devon Rural Housing Association
South Hams District Council
Sovereign Housing Association Limited
Splitz Support Services
Stop Abuse For Everyone
Teign Housing
Teignbridge District Council
The Women's Centre Cornwall
Together Drug & Alcohol Service (EDP)
Torbay & South Devon Healthcare NHS Foundation Trust
Torbay Council
Torbay Domestic Abuse Service (TDAS)
Torbay Education Safeguarding Service (TESS)
Torbay Youth Offending Team
Torridge District Council
University Hospitals Plymouth NHS Trust
We Are With You - Cornwall
West Cornwall Womens Aid
West Devon Borough Council
West Exe Nursery School
Westward Housing Group
WILD - Young Parents' Project
Willow Tree Housing Partnership

3.2. The Partners within this protocol subscribe to the following:

- The agreed standards must provide safeguards and an appropriate framework for the controlled exchange of timely, accurate and relevant information.
- The General Data Protection Regulation and Data Protection Act 2018 principles, along with the common law principles of confidentiality, must be upheld.
- The rights of the data subject under the Human Right Act 1998 and Article 8 of the European Convention on Human Rights are to be upheld.
- This Agreement will be reviewed biennially, or in the light of new legislation or guidance.
- Any partner may request any change to the Agreement at any time by submitting to the Agreement holder a suggested revision.
- The nominated holder of this Agreement is the Head of Information Management, Devon and Cornwall Police, who shall, on behalf of the partnership:

- ensure that a review is carried out when required;
- circulate all requests for change, co-ordinate responses, obtain agreement for the changes from the partnership and distribute codes of practice and guidance as these become available.

4. Definitions

4.1. For the purpose of this Agreement, the following terms are defined as:

- **Caldicott Guardian** is a role within the NHS and Social Services which has responsibility for protecting and using patient/client identifiable health and care information.
- **Data Subject** within this protocol will be a victim or the alleged offender of domestic abuse and sexual assaults who has reported an incident to one of the partners to the protocol.
- Domestic Abuse is any incident, or pattern of incidents, of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are, or have been, intimate partners or are family members, regardless of gender or sexuality. This includes:
  - physical, sexual, financial and emotional abuse;
  - stalking;
  - so-called 'honour-based' or 'honour' violence and forced marriage;
  - female genital mutilation;
  - coercive and/or controlling behaviour.
- **MARAC** is the Multi-Agency Risk Assessment Conferences.
- **Non-Secure Internet Link** is any email traffic that is not transmitted via two secure email addresses.
  Established email domains that will enforce encryption include email addresses to and from .gov.uk, .pnn.police.uk and nhs.net.
  Confirmation from the IT Security Officer or equivalent that encryption is enforced is required by the sharing partner if an alternative email domain is used. Secure email solutions can also be used if available, e.g. Egress, however emails should not be sent to personal email accounts such as Gmail, Hotmail, Yahoo etcetera.
- **Prevention of Offending** is an activity which reduces the likelihood of offending/reoffending through the provision of relevant information that reduces the risk factors associated with offending and promotes protective factors.
- **Personal Data** means any information relating to an identified or identifiable natural person, the data subject, who can be identified from data, or from data and other information which are in the possession of, or are likely to come into the possession of, the data controller. They include, without limitation, any expression of opinion or intentions in respect of such a living individual.

Reference GDPR Article 4 (1).

- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the

purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Reference GDPR Article 4 (7) and DPA Part 3, Chapter 1 (32) (1).

- **Processor** in relation to personal data, this means any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
  Reference GDPR Article 4(8) DPA Part 3, Chapter 1 (32) (3).
- **Sexual Assaults** are any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, acts to traffic someone's sexuality, using coercion, threats of harm or physical force, by any person, regardless of their relationship to the victim, in any setting including, but not limited to, home and work.
- **Consent** refers to freely given, specific, informed and unambiguous indication of their wishes by which he or she, by a statement, or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent is to give permission for the partner agency, as the 'data owner' to give information from their records to the agencies working within the local Scheme. A copy of this consent form (See Appendix 2) will be attached to the individual's record and copied to the receiving agency when information is disclosed.
- Devon and Cornwall Police are a competent authority under Part 3 DPA 2018. As a competent authority, Devon and Cornwall Police process data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

5. Detailed Standards

5.1. Scope

This Agreement can cover the exchange of information at MARACs or between the nominated officers within the partner organisations. It will relate to incidents reported within the Devon and Cornwall areas, or where very high risk victims have relocated to Devon or Cornwall to escape abuse.

5.2. Registration/Notification

Each partner will ensure that they are notified under the General Data Protection Regulation and Data Protection Act 2018 to receive and process personal data. Data to be transferred will include some special categories of personal data information. It will therefore be necessary at the registration stage, where disclosure is likely without consent, to select criteria for processing from Article 9 of the GDPR 2018 or Schedule 8 of the Data Protection Act 2018 and the further legal issues contained within Appendix 1.

5.3. The Vital Interest of the Data Subject and Public Safety

A partner's responsibility for public protection may at times clash with the responsibility of confidentiality to the individual. Similarly such action can be taken in the vital interests of the data subject, e.g. where there is no public interest, under a Court Order or under a statutory obligation to disclose information. Prior to disclosure, including disclosure at MARAC or for high risk sexual assault cases, the nominated officer must consider whether the personal information is held under a duty of confidence and whether there is an overriding public interest or other justification for disclosing the information, thereby treating the disclosure of information as an exception to the general principles of confidentiality. This will apply even where the individual has refused consent for information to be shared however, each disclosure must be treated on a case-by-case basis.

No disclosure relating to the alleged offender will be made to the voluntary sector partner without the offender's written consent, unless required where the public interest outweighs the presumption of confidentiality and where disclosure will preserve public safety and/or prevent or detect crime (see Appendix 1). In these circumstances, regard must be given to the fact that such disclosure amounts to an exception to the general principle of confidentiality.

Details of witnesses or non-victim reporting persons must not be disclosed without their written consent.

5.4. **Requesting/Disclosing Personal Data**

It is essential that adequate control of the flow of data be maintained. The General Data Protection Regulation and Data Protection Act 2018 permits the exchange of data, provided the data has been fairly obtained and processed, i.e. the individual has been clearly informed how their data will be used and disclosed, and it is appropriately notified under the Act. However, disclosures can also take place under certain circumstances where the data protection principles will not apply - under the Act's non-disclosure exemptions. Reliance on these must be assessed on a case-by-case basis, the exemptions include:

- To protect the vital interests (GDPR Article 6(1) (d)) of the individual or relevant third party, where consent cannot be given or is withheld. It is accepted that in exceptional circumstances (e.g. for the purposes of safeguarding the victim and/or agency staff against proven high risk of abuse) any specific voluntary sector partner may receive personal information without, or against the consent, of the data subject.
- At the request of and/or with the consent of the individual concerned. Engagement with a Voluntary Sector partner would normally arise from consented disclosure. Except in the circumstances as above – protecting vital interests – the D & C Police Victim Care Unit make referrals to support services under the Code of Practice for Victims of Crime which includes Victim Support and other organisations who provide support. Disclosures relating to Domestic abuse and sexual assaults are not to be made to Voluntary Sector under this Protocol, unless the victim has provided express consent at the time of the initial

crime report, or has amended the initial record by subsequent recorded consent. However, similarly consent to disclose to any voluntary sector or non-statutory partner must be evidenced within the individuals file.

- Additionally, at a later stage, prior to a Multi-Agency Risk Assessment Conference taking place, a victim will be informed by their allocated IDVA that their information will be discussed in a multi-agency MARAC meeting. Any objections to their information being shared should be recorded by the IDVA along with a rationale why the victim's wishes for disclosing are being overridden where a multi-agency safeguarding approach is necessary for the high-risk victim.
- For the prevention or detection of crime, the apprehension or prosecution of offenders and taxation purposes, the disclosure of pertinent and relevant information must be on a case-by-case basis and where failure to provide the information would be likely to prejudice these purposes. For this provision to apply there would have to be a substantial risk of prejudice, rather than a mere chance. All requests and responses must be appropriately authorised and documented.
- Where a disclosure is made in connection with legal proceedings for the purpose of obtaining legal advice and establishing, exercising or defending legal rights.

Procedures for the handling of requests/disclosures of information can be found in Appendix 3 – The Working Practice Agreements for dealing with domestic abuse and sexual violence.

5.5. **Nomination of Staff**

In order to comply with the principle of security and the common law duty of confidentiality, this Agreement contains a list of appropriate nominated contact persons. Each partner organisation will provide details of:

- whom contact should be made with in relation to this Agreement;
- whom requests for information should be sent to;
- whom disclosures should be made to;
- who are responsible for data protection and security compliance for their organisation.

Requests from unauthorised organisations or staff will be declined. The Disclosure of Information from the Health Service agencies must be endorsed by the relevant Caldicott Guardian.

Partner organisations are to determine how to maintain up-to-date and accurate records of key contacts and to keep the owner of this ISA up to date with those changes.

5.6. **Accuracy of Data**

Each partner has a responsibility to maintain the accuracy of data supplied under this Agreement. There is a statutory duty in the General Data Protection Regulation and law enforcement processing under the Data Protection Act 2018 for any partner supplying personal data to verify the information and

advise the recipients if the data supplied is subsequently found to be inaccurate.

Where an inaccuracy is discovered after a disclosure has been made, it will be the responsibility of the party discovering the inaccuracy to bring this to the notice of the data controller in writing as soon as is practically possible, who should then notify all recipients of the correction.

To meet this responsibility, partners are expected to keep a record of disclosures to indicate that a disclosure has been made and to inform recipients of disclosures if they become aware of any inaccuracies which may prejudice the rights and freedoms of, or detrimentally affect, the data subject or individual.

5.7. **Confidentiality and Security**

Each partner organisation shall, at all times, keep all personal data supplied as confidential pursuant to this Agreement, and any publication of data supplied pursuant to this Agreement will not identify any individual 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. This clause shall survive termination of the Agreement or the withdrawal or removal of any partner. Reference GDPR Article 4 (1).

Each partner will take all reasonable steps to adequately protect the data from both a technological and physical point of view, this includes manual files and transfers of data between partners. The Police will grade the information provided to them to restrict access where this is applicable.

Any breach of confidentiality, or incident involving a risk or breach of the security of information, should be notified to the designated Data Protection/Information Assurance Manager of the relevant organisation without delay to ensure this is dealt with in accordance with their respective policy, procedures and the indemnity for this Agreement.

If any information which is shared under this Agreement is lost, stolen or disclosed to anyone who should not have had access to it, this shall be a breach of this Agreement.

The Data Protection Officer for the breaching party must notify the other party of any breach by the breaching party as soon as it becomes aware of the breach. If there is suspicion of a breach, this also must be notified immediately.

5.8. **Circulation, Retention and Destruction of Data**

Partners agree that all received disclosures will be securely handled and stored, only circulated to those who are entitled to receive the information and that the person or organisation receiving the information has adequate safeguards and working practices in place to prevent the dissemination of disclosures to parties not entitled to receive them.

Partners agree that all disclosed information will be retained for no longer than necessary and only in relation to the purpose for which such information was disclosed, following which, all disclosed information will be securely disposed of or erased.

Devon and Cornwall Police may, at any time, audit disclosures that have been made to establish what information is still held and which has been securely disposed of or erased, and by which secure method disposal took place.

In order to meet their obligations under this section, all partners are expected to introduce a procedure and nominate a person to conduct reviews of personal data received through a disclosure on a regular basis and at least every six months.

5.9. **Data Subject Requests**

Individuals have the right to request access to a copy of all information held about them on computer and manual files, unless an exemption applies where information can be withheld under certain circumstances. Individuals also have the right to request erasure, rectification, restriction, data portability and to object. Partners will adopt common procedures for dealing with requests under the data protection rights. See Appendix 4 for procedures on handling requests for individuals' access to information.

5.10. **Complaints**

Any complaint made will be brought to the attention of the nominated person of the relevant partner, and will be dealt with in accordance with their own policies and procedures. Partners will keep each other informed of developments following a complaint received, where relevant.

5.11. **Compliance and Good Practice**

Any further guidance or codes of practice should be reviewed biennially and distributed via the Agreement holder for consideration and possible attachment to this Agreement.

5.12. **Equality Act 2010**

The assessment of relevance and impact of this Agreement in relation to the public authorities' general duty under the Equality Act is the individual responsibility of the signatories.

5.13. **Publication of Agreement**

i. This Agreement may be published by each of the signatories in accordance with their respective obligations under the Freedom of Information Act [FoIA] 2000. No section of the Agreement is currently classed as Closed under Freedom of Information apart from the contact details of each contact and nominated officer. These are held on a separate contacts list which will be distributed amongst the partners along with the signed final version of the ISA and will not be published within the protocol under FoIA.

ii. The Durant Ruling of the Court of Appeal (Civil Division) in December 2003 has indicated that, in relation to this Agreement, data linked to an

individual's role, e.g. role title and contact number, is not personal information.

6. Indemnity

By signing up to this Agreement, each partner shall be fully indemnified by the other partners in accordance with the following:

i The parties hereto are working in partnership in exercising in their functions and their responsibility for the protection of the public.
ii This Article provides guidance on the exchange and use of personal information.
iii Further, the parties have agreed to indemnify one another in the manner described below in circumstances where a person who is the subject of information exchanged between any of the parties, in accordance with the Article, suffers loss as a result of the misuse or inaccuracy of the information and brings an action claim or demand as a consequence thereof.
iv In respect of the indemnity, the parties have agreed as follows:

Provision of Information

a In consideration of the provision of information in accordance with this Agreement the parties hereby undertake to indemnify, and keep indemnified, each other against all loss, damages or liability (whether criminal or civil) costs, charges and expenses, including legal fees and costs, at any time incurred or suffered by a party to this Agreement arising on, or out of, the misuse of information provided in accordance with the Agreement. Provided that such indemnity may only be invoked in the circumstances set out in sub-clauses (b) to (c) below.
b The party seeking the indemnity may only seek to enforce it against the party that supplied or misused the information in accordance with this Agreement.
c The party claiming the benefit of the indemnity has notified the party against whom it intends to invoke the indemnity within 14 days of any third party action claim or demand ('the claim'), thereafter the parties shall consult as to how the party against whom the claim has been made ('the defendant') should proceed in respect of such claim.
d In the absence of contrary agreement between the parties, the defendant shall resist the claim as far as final judgement. In the event of any claim being paid or compromised, or in the event of final judgement being given against the defendant, the party against whom the indemnity is being invoked will, within 14 days of being so notified by the defendant, reimburse the defendant with the full amount of such payment or final judgement payment to cover those costs and expenses identified in clause (a) above. Provided always that where any claim is paid or compromised, the party against whom the indemnity is being invoked shall have the right to be consulted as to the extent of any payment.

e The party seeking to invoke the indemnity may not do so if it has made, or makes, any admission which may be prejudicial to the defence of the action claim or demand.

By signing the Certification in Section 6 the partners accept and will adopt the detailed standards included in this Agreement at Section 4 and this Indemnity, and agree to maintain the specified standards. In addition the partners will not use, release or otherwise disclose any data whatsoever:

a for any other secondary use not specified under this Agreement or by regulations made there under; and/or
b to any organisation which is not a signatory to this Agreement.

7. Certification – Agreement for the Exchange of Information

By signing below, the signatories:

- accept and will adopt the statements included in this Agreement and the indemnity;
- agree to maintain the specified standards;
- agree not to use, release or otherwise disclose any data whatsoever outside of this Agreement;
- are controllers in their own right under data protection in relation to the data shared by them under this agreement until the point when the information is shared when data controller responsibility transfers to the recipient of the data;
- hold a valid registration with the Office of the Information Commissioner (ICO);
- confirm that the signatory has informed all colleagues and that the colleagues have read, understood and agree to the terms of the Agreement.

It is recommended that signatories retain a list of those colleagues who have read, understood and agree to the terms of this agreement.

Organisation .....

Name (print) .....

Position .....

....

Signature **Date**

8. Version Record

Corporate Version	Amendment	By	Date
0.1	First draft composed.	G. Stoneman	19-Nov-19
0.2	TF answers to queries from V0.1 added.	G. Stoneman	13-Feb-20
0.3	GBs partner list and comment answers updated.	G. Stoneman	16-Mar-20
0.4	Police logo updated. Clause 2 – Powers inserted. Partners updated and list of those without contact details produced. Bullet points four and five added to certification.	G. Stoneman	11-Jun-20
0.5	Appendix 3 –Wording inserted to reflect Cornwall method for sharing using online case management system -Halo Page 7/8 Requirement to send a letter to a victim removed. IDVA to liaise with victim to inform them of multi-agency sharing	T. Furbear	13-Aug-20
0.6	Partner list updated, with Crown Prosecution Service, National Probation Trust, Victim Support and Youth Offending Team all removed. Refuge4Pets added 05-Dec-23.	G. Stoneman	18-Aug-20

Appendix 1 | Legal Issues – Lawful Basis for Processing

This Agreement is focused on the sharing of information in domestic abuse and sexual assault cases. Within this process signatories can utilise the conditions within GDPR Article 6 and DPA 2018 Schedule 8, Section 35(5) to make disclosures without consent for high-risk cases, where this is required to protect the vital interests of the data subject or others or where disclosure is necessary for the prevention or detection of crime.

If processing special category data from Part 3 into Part 2 of the Data Protection Act 2018, an additional condition for processing special category data under Article 9 of GDPR must be met.

Outside of this high-risk case scenario, information provided by the data subject to the receiving agency would have been deemed provided in confidence and, where it is necessary to share personal data within the partners, any disclosure should be with the informed, explicit, written consent of the data subject or it must be capable of being justified as an exception to the general Common Law Duty of Confidentiality and the General Data Protection Regulation and Data Protection Act 2018.

In the case of personal data held under a duty of confidence, a disclosure may be made in respect of that personal data if there is a compelling reason of overriding public interest or another overriding statutory justification which permits the disclosure.

The signatories understand the public interest criteria to include, but not be limited to:

- the administration of justice;
- maintaining public safety;
- the apprehension of offenders;
- the prevention of crime and disorder;
- the detection of crime;
- the protection of vulnerable members of the community.

The signatories should confirm, check and verify the following points when deciding if the public interest criteria should override any duty of confidentiality:

- That the intended disclosure is proportionate to the intended aim.
- The vulnerability of those who are at risk where this is a factor to support the disclosure?
- The likely impact of the disclosure on the offender.
- That there is no other equally effective means of achieving the same aim.
- That the disclosure is necessary to prevent or detect crime and uphold the rights and freedoms of the public.
- That the disclosure of the information is necessary to protect other vulnerable people.

When considering or making any disclosure, the signatories should ensure they are compliant with Article 8 of the Human Rights Act 1998. This states that everyone has the right to respect for his private and family life, home and his correspondence and

that there shall be no interference by a public authority with this right except, as in accordance with the law and is necessary in a democratic society, in the interests of:

- national security;
- public safety;
- economic wellbeing of the country;
- the prevention of crime and disorder;
- the protection of health and morals; and/or
- the protection of the rights or freedoms of other.

The signatories should confirm, check and verify relevant guidance issued by the Home Office and other Government departments when considering and/or making any disclosures.

Data protection and confidentiality issues surrounding a disclosure will not apply if the consent of the individual has been sought and obtained.

Within the current domestic abuse working practices of the Devon & Cornwall Police, the provision of consent is sometimes recorded in a tick-box within an electronic record by an officer who has obtained consent The Police are currently content with this process as an adequate record to indicate the victim's consent to information sharing to reduce the risk of further incidents of domestic abuse, however the remaining principles within the General Data Protection Regulation and Data Protection Act 2018 must be adhered to by all parties to this protocol.

Legal Powers Supporting Information Sharing within this Protocol

General Data Protection Regulation Article 6

The GDPR conditions required to process the personal information linked to this Agreement are:

- 6(1) (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- 6(1) (d) Vital interests: the processing is necessary to protect someone's life.
- 6(1) (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.
- 6(1) (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. (Note: Legitimate Interest cannot apply where the Police are processing data to perform an official task).

Data Protection Act 2018 Schedule 8, Conditions for Sensitive Processing

a With the explicit consent of the data subject, or,
b (Schedule 8, 4 (1) (a)(b)) the processing is necessary for the purposes of:

    - protecting an individual from neglect or physical, mental or emotional harm;
    - protecting the physical, mental or emotional well-being of an individual;

- the individual is aged under 18, or aged 18 or over and at risk, or

a (Schedule 8, 4 (2) (a)(b)(c)) the processing is necessary for reasons of substantial public interest and:

- consent to the processing cannot be given by the data subject, or
- the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, or
- the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the vital interest of another person.

Crime and Disorder Act 1998

Under Section 17 the relevant authority has the duty to consider crime and disorder implications and the need to do all that it reasonably can to prevent:

- crime and disorder in its area, including anti-social and other behaviour adversely affecting the local environment;
- the misuse of drugs, alcohol and other substances in its area; and/or
- re-offending in its area.

Under Section 115(1) – Any person who would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority, shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.

The Code of Practice on the Management of Police Information

Reference 4.1 – Authorised Professional Practice on the Management of Police Information issued by the College of Policing ("APP") and the Code of Practice for Management of Police Information. This sets out principles governing the management of police information, including procedures governing authorised sharing of information obtained and recorded for policing purposes within the police service, and with other agencies.

Policing purposes are defined within the code as:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice; and
- any duty or responsibility of the Police arising from common or statue law.

The Code allows the Police to disclose police information to other persons or bodies where this is reasonable and lawful to do so for policing purposes as set out above. Any sharing of information must comply with the College of Policing Authorised Professional Practice (APP) Management of Police Information (MOPI) and any protocol, national or local, which may be agreed with the persons or bodies needing to receive the information.

Additionally the MOPI sets out obligations on the persons or bodies receiving police information which equate to the detailed standards set out in Sections 4.1 to 4.11 of this Agreement.

Common Law Duty of Confidence

In the case of personal data held under a duty of confidence, a disclosure may be made in respect of that personal data if there is a compelling reason of overriding public interest or another overriding statutory justification which permits the disclosure.

The signatories understand the public interest criteria to include, but not be limited to:

- the administration of justice;
- maintaining public safety;
- the apprehension of offenders;
- the prevention of crime and disorder;
- the detection of crime; and/or
- the protection of vulnerable members of the community.

The signatories should confirm, check and verify the following points when deciding if the public interest criteria should override any duty of confidentiality:

- That the intended disclosure is proportionate to the intended aim.
- The vulnerability of those who are at risk where this is a factor to support the disclosure?
- The likely impact of the disclosure on the offender.
- That there is no other equally effective means of achieving the same aim.
- That the disclosure is necessary to prevent or detect crime and uphold the rights and freedoms of the public.
- The disclosure of the information is necessary to protect other vulnerable people.

When considering or making any disclosure, the signatories should ensure they are compliant with Article 8 of the Human Rights Act 1998, which states that everyone has the right to respect for his private and family life, home and his correspondence, and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

- national security;
- public safety;
- economic wellbeing of the country;
- the prevention of crime and disorder;
- the protection of health and morals; and/or
- the protection of the rights or freedoms of others.

The signatories should confirm, check and verify relevant guidance issued by the Home Office and other Government departments pursuant to, or in respect of the Acts or laws referred to in this section from time to time provided that, in the event of

any conflict between such guidance and the relevant Act(s) or laws then the Act(s) or laws (as may be appropriate) will prevail.

The Human Rights Act 1998

Section 8(1) – All data subjects have a right to a private family which can only be interfered with if justified and proportionate.

Interference with this right may be justified where the processing is necessary and in the interest of:

- discharging the common law police duties;
- preventing / detecting unlawful acts;
- protecting public against dishonesty;
- preventing fraud;
- terrorist finance / money laundering;
- safeguarding children and adults at risk; and/or
- safeguarding economic wellbeing of vulnerable adults.

Appendix 2 | Consent Form
(to be produced on Headed Paper of the Partner seeking consent)

Consent for sharing of data held within the [Insert Specific Partner] records
The agencies listed below are working together to reduce the incidence of domestic abuse, sexual assaults and to provide multi-agency support to those victims. I wish to take support and benefit from this scheme and I give my freely given, specific, informed consent for my personal data relating to incidents of domestic abuse and sexual assault, in which I am a victim/survivor to be shared with the following listed agencies;

I do not wish information to be provided to any agency listed below

_____

I have been made aware that where a statutory power to share information exists certain information may disclosed without my consent.

This Agreement complies with the requirement for explicit consent to be given under Article 7 of the General Data Protection Regulation 2018.

....
Signature **Date**

Appendix 3 | The Working Practice Agreements for Dealing with Domestic Abuse and Sexual Violence

The Working Practice Agreement for Sharing Information to deal with Domestic Abuse and Sexual Assault at MARACs

1. Disclosure via end-to-end secure email is a secure method of the delivery of the requested information (see Section 5.4 Requesting/Disclosing personal data). This will ensure that accurate information is passed directly to the requesting partner or person and that an audit trail is established.

   For Cornwall, all information in relation to MARAC cases is stored and shared between MARAC representatives via a secure, online, electronic case management system, HALO. Access to said information is restricted to allocated and trained MARAC representatives and the data controllers; the domestic abuse and sexual violence team and the data analyst team at Cornwall Council. User activity is monitored and can be tracked if necessary.

2. The signatories should respond to formal requests for disclosure of personal data within two working days of receipt of the request. However, it is acknowledged that there may be occasions when the disclosure is required more urgently.
3. Disclosures at Meetings

   - Signatories who anticipate making disclosures at meetings should ensure they are empowered to do so and that such disclosures are permitted by all relevant legislation.
   - Such disclosures should be recorded within the Minutes of the relevant meeting and the relevant signatory or signatories shall ensure that these Minutes are retained for at least six (6) years.
   - It is suggested as a model of good practice that those signatories making disclosures at meetings should clarify all issues reasonably relevant to any intended disclosure to include, without limitation, confidentiality issues and powers to make the disclosure prior to the commencement of the relevant meeting.

Working practice for dealing with other high risk information:

- High-risk information can be shared with or without consent (GDPR 2018 Article 6 1(d)). Please see the above Agreement for what constitutes high-risk.
- This will be shared in the most efficient way possible depending on the case.
- Information will only be used for the purpose(s) for which it was requested, it will be securely stored and destroyed under confidentiality conditions when no longer required.

Where appropriate and possible, explicit consent should be obtained from the data subject for the disclosure to take place in accordance with GDPR 2018 Article 6. This consent must be freely given and obtained free from any form of duress, threat or fraud. Consent to share information should be recorded on the partner organisation's client records. Further guidance about consent can be found via the Information Commissioner's Office (ICO) website. If consent cannot be gained, the grounds on which consent can be overridden must then be considered. Disclosure of special

categories of personal information can be gained if this is in the defined category of public interest. This is when decisions are made after consent has been refused, is withheld or is unknown, i.e. where it has not been possible to contact a victim, and if there is an overriding public interest (see Common Law Duty of Confidentiality Appendix 1 above). Any disclosure of Special Categories of personal information will be restricted to the minimum necessary to achieve the purpose. Documentation of the decision-making process will be stored together with a copy of the information shared.

Working practice for sharing medium and standard risk information:

- Medium and standard risk will only be shared with consent. This may be on a referral or information request basis.
- The information shared should not be disclosed to any third party without the written consent of the agency and client that provided the information.
- It should be stored securely and deleted when it is no longer required for the purpose for which it is provided.

Appendix 4 | Procedures for Handling Right of Access (Subject Access Requests)

1. All signatories should have internal procedures in place for handling and responding to Subject Access Requests, i.e. requests for access to Personal Data made pursuant to GDPR Article 15 and DPA 2018 Part 3, Chapter 3.

2. The following procedures should also be used for dealing with Subject Access Requests in respect of personal data:
    - If on receipt of a Subject Access Request the request refers only to personal data processed by the signatory receiving the request, that signatory should follow its own standard procedures for dealing with such requests.
    - If on receipt of a Subject Access Request the request refers to any personal data which originated from another signatory, it will be the responsibility of the signatory receiving the Subject Access Request to contact the signatory from whom the personal data originated, via the nominated contact person, to determine whether they wish to claim an exemption to withhold the personal data under the provisions of the General Data Protection Regulation or Data Protection Act 2018.
    - Any decisions made to withhold personal data from a data subject should be taken with care and, if necessary, legal or other appropriate professional advice sought. They should also be formally recorded in case of subsequent dispute. There is no requirement to inform the data subject requesting access that personal data has been withheld from them for these purposes.

3. Third Party Information

    When a signatory cannot comply with a Subject Access Request without disclosing information relating to another individual who can be identified from that information, the provisions of GDPR Article 15 or Chapter 3 (Rights of the Data Subject) sections 43 to 45 of the Data Protection Act 2018 shall govern whether or not the disclosure is made to the data subject making the Subject Access Request.

4. Time Limit for Dealing with Subject Access Requests

    Subject Access Requests must be dealt with as quickly as possible in order to ensure that responses to them are made within the one calendar month period required by statute. The one calendar month period commences from the date that sufficient information is received from the data subject that enables the signatory to process the Subject Access Request.