Department of Justice
www.justice-ni.gov.uk

DOMESTIC VIOLENCE AND ABUSE DISCLOSURE SCHEME NORTHERN IRELAND (DVADS NI) GUIDANCE

March 2018

Contents

Sections:

Domestic Violence and Abuse Disclosure Scheme Northern Ireland

- Guidance

This document contains operational guidance on the Domestic Violence and Abuse Disclosure Scheme Northern Ireland, introduced by the Department of Justice (DoJ) on 26 March 2018.

The guidance is non-statutory and should not be regarded as authoritative legal advice.

If you have any queries regarding this guidance, then you should contact DoJ at:

Community Safety Division
Safer Communities Directorate
Block A, Castle Buildings
Stormont
Belfast
BT4 3SX

Telephone: 028 90 528102
Email: dvads@justice-ni.x.gsi.gov.uk

This guidance is also available on the Department of Justice website:
www.justice-ni.gov.uk

Section 1: Introduction

1.1 Domestic violence and abuse is a significant problem in Northern Ireland and as such, it is a key area which the Department of Justice (DoJ), in conjunction with its statutory partners, is committed to addressing. Latest statistics show that during 2016/17, there were over 29,000 domestic violence and abuse incidents reported to the Police Service of Northern Ireland[1], with almost 14,000 crimes committed.

1.2 In March 2016, the new joint DoJ and Department of Health seven year Strategy 'Stopping Domestic and Sexual Violence and Abuse', was published. The principal aim of the strategy is to put an end to domestic violence and abuse[2] in Northern Ireland, which is to be achieved through delivery of a number of strand objectives and key actions. Strand 2 of the strategy focuses on prevention and early intervention and the introduction of a Northern Ireland Domestic Violence and Abuse Disclosure Scheme (DVADS) has been set as a key action against the delivery of this objective.

Section 2: What is DVADS?

2.1 Police across the United Kingdom have a common law power to disclose relevant information to members of the public when it is necessary to do so to prevent crime. In Northern Ireland, police have the additional power, under section 32 of the Police (Northern Ireland) Act 2000, to *protect life and property* and *to prevent the commission of offences*[3].

2.2 DVADS has been developed as a specific mechanism to assist police in delivering its existing powers and to consider the disclosure of information in the domestic violence and abuse context. It will allow police and its partners, to better manage risk through the sharing of relevant information about one person's history of domestic abuse with another, or to a third party deemed best placed to safeguard that person.

2.3 **The principal aim of DVADS is to keep people safe, by helping protect potential victims, and allowing them to make an informed choice on whether they would wish to continue in their relationship.** It focuses on identifying the level of risk and managing the risk through disclosure of information.

[1] 'Domestic Abuse Incidents and Crimes Recorded by Police in Northern Ireland', PSNI statistical report, period ending 31 March 2017.

[2] Domestic violence and abuse is defined in the Strategy as: *'threatening, controlling, coercive behaviour, violence or abuse (psychological, virtual, physical, verbal, sexual, financial or emotional) inflicted on anyone (irrespective of age, ethnicity, religion, gender, gender identity, sexual orientation or any form of disability) by current or former intimate partner or family member'.*

[3] subsection (1)

2.4 Given existing police powers to disclose, the operation of DVADS does not require specific legislation of its own to operate.

2.5 That said, any disclosure considered under DVADS must have due regard to the legal powers and obligations of the Human Rights Act 1998 - particularly Article 2 (right to life), Article 3 (prohibition of torture), Article 6 (right to fair trial) and Article 8 (right to private and family life, including physical and psychological integrity), which will be engaged - as well as the Data Protection Act 1998, including the forthcoming General Data Protection Regulation [and relevant case law, including the case of Osman v United Kingdom]. This helps ensure that disclosure considered and made is done within the confines of the law, and that information relayed is necessary and proportionate to the risk identified to the potential victim. More on this particular point will be discussed later.

Section 3: Background to DVADS

3.1 Disclosure schemes, similar to DVADS operate across neighbouring jurisdictions of the UK, as well as internationally.

3.2 The concept was first introduced in England and Wales in March 2014 – the 'Domestic Violence Disclosure Scheme' (DVDS) - and it is more commonly known there as 'Clare's Law'. Clare's Law follows the murder of Clare Woods in Greater Manchester in 2009 by her former partner, where Clare had no knowledge of her partner's past misdemeanours.

3.3 Following the introduction of DVDS in England and Wales, a similar scheme was developed and introduced in Scotland in October 2015 – the Disclosure Scheme for Domestic Abuse Scotland (DSDAS). Practice extended further to international jurisdictions a little later, with the introduction of a national scheme in New Zealand in December 2015, and a two year pilot across four police areas in New South Wales, Australia in March 2016. Currently, no scheme operates, or is planned for introduction, in the Republic of Ireland.

3.4 In developing DVADS, DoJ considered the frameworks of schemes established across those jurisdictions, consulting closely with its partner agencies, to help ensure that the Northern Ireland model meets the specific needs of victims in this jurisdiction.

Section 4: Overview of practice

4.1 It should be noted that only individuals aged 16 years and over are applicable for this scheme – this includes those who may apply to the scheme, or those who may be subject of a disclosure. The PSNI Public Protection Branch (PPB) will be responsible for operating DVADS. It is considered that PPB officers have the appropriate skills and knowledge to manage domestic violence offenders, as well as investigating domestic violence and abuse incidents.

4.2 DVADS recognises two ways to disclose information: **'Right to Ask'** and **'Power to Tell'** – a flow chart demonstrating the key processes relevant to each pathway is included at Annex B:

- **'Right to Ask'** is triggered when a person (member of the public) makes a direct application to PSNI for information about an individual whom they suspect may have a history of violent or abusive behaviour towards a previous partner and where there are concerns about that individual's current behaviour.

- **'Power to Tell'** is triggered when PSNI receive indirect information or intelligence about a person thought to be at risk from a partner, and where, after appropriate checks are made, PSNI judge that a disclosure should be made to safeguard that person.

4.3 More detailed information regarding the above is provided later in the guidance (Section 7 – the disclosure process).

4.4 It should be highlighted that the scheme does not replace existing arrangements for Disclosure and Barring Service checks or Freedom of Information requests. If it is identified, at the initial contact with a person accessing the scheme, that the request is one of these other types of enquiry, then it should be directed through the existing route for that type of request.

4.5 DVADS may overlap with and complement other disclosure processes, such as the Public Protection Arrangements Northern Ireland (PPANI) and the Child Protection Disclosure Arrangements Northern Ireland (CPDA). Consideration should be given to which process is the most appropriate in each case, dependent on the individual circumstances of the case.

4.6 Critical to the success of the scheme is the need to assess risk at each stage of the disclosure process, as this will help inform the practical actions necessary to safeguard the potential victim, and inform the development of a potential disclosure.

4.7 A key element of the disclosure scheme is ensuring that potential or actual victims of domestic violence and abuse are protected from harm. Protection should also be afforded to any previous victim or a third party making an application that may be identified at risk, as a direct consequence of the scheme. By making a request for disclosure, a person will often also be registering their concerns about possible risks to their own safety, or that of another individual. It is, therefore, essential to this process that police work closely with the local Multi-Agency Risk Assessment Conference (MARAC), to ensure that any possible risks of harm to the potential victim are fully assessed and managed.

Section 5: DVADS benefits

5.1 DVADS provides the following benefits:

a) Introduces recognised and consistent procedures for disclosing information that enables a partner who is/was in relationship[4] with a previously violent or abusive individual to make an informed choice about continuing in that relationship, or about their personal safety if no longer in the relationship;

b) Enhances the previous arrangements, whereby disclosure occurred largely in a reactive way, when agencies came into contact with information about an offender having a history of previous violence;

c) Under 'Right to Ask', a concerned person whether the partner or a third party (person known to the potential victim who has a concern about that person's safety), can now proactively seek information, with an expectation that the agencies responsible for safeguarding victims of domestic violence and abuse will check to find out whether relevant information exists and if it does, that consideration will be given to its disclosure, where necessary and proportionate to protect the potential victim;

d) Under the 'Power to Tell', where a safeguarding agency comes into the possession of information about the previous violent or abusive behaviour of an individual that may cause harm to a potential victim, members of the public can now expect the safeguarding agency to consider whether any disclosure should be made and to disclose information if it is lawful i.e. if it is necessary and proportionate to protect the potential victim from crime.

Section 6: Purpose of guidance

6.1 The purpose of this guidance document is to provide police officers, particularly those who work in the area of public protection, who will be responsible for the scheme's operation, and partner agencies who will be involved in the Decision Making Forum (DMF) process (see later), with information concerning the practical application of the scheme.

6.2 It is important to remember that the purpose of DVADS is to facilitate disclosure in order to protect a potential victim from harm. Each request for information under the scheme should be considered on a case-by-case basis and police should seek legal advice, as may be necessary. There may be occasions, for

[4] A relationship is where the persons are 'personally connected' i.e. where both individuals are, or have been a couple, or otherwise in an intimate personal relationship with each other. This relationship does not necessarily have to involve a sexual element.

example, when information cannot be disclosed in accordance with the scheme, but where disclosure may still be possible under a different route.

6.3 Definitions of terms used in this guidance are at Annex C and principles underpinning the scheme are set out at Annex D.

6.4 In applying the processes of the scheme, officers must be alert to the impact of domestic violence and abuse on any children specified in the DVADS application. The recognition of children who may be at risk (domestic violence and abuse or otherwise) is the responsibility of all officers involved at each stage. In circumstances where child protection matters are identified the information will be passed to the relevant Social Services Trust in written form as soon as possible. Article 3(1) of the UN Convention of the Rights of the Child, should also be observed.

6.5 If a child is a member of the household or 'A' is pregnant, the Duty Social Worker should be informed if there are immediate concerns in respect of the welfare, protection or control of a child. In the absence of any immediate risk, details should be passed to the relevant local HSC Trust Gateway team as soon as possible.

6.6 Police officers should advise 'A' that it is police policy to share information with the local Family and Child Care Manager where children are resident or present at the home or where the victim is pregnant. If it is known that the subject has children elsewhere, HSC Trust Gateway team should also be advised.

Section 7: The Disclosure Process

Right to Ask

7.1 'Right to Ask' follows a *three step* process by police before referral is made by PPB to a DMF. The total timescale for this strand of the scheme is 45 days for non-urgent cases (from receipt of an application, until disclosure is made). Where an urgent need for disclosure has been identified (such as potential violations of Articles 2 or 3 ECHR), PSNI will seek to deal with the disclosure request as quickly as possible.

Maximum Timescales[5] for DVADS				
	Right to Ask - submission of application form		**Power to Tell** - receipt of indirect information	
Step 1	First contact made with applicant and initial police checks carried out	To be completed within 3 days from receipt of application form		
Step 2	Face-to-face meeting with applicant, completion of DASH risk assessment and implementation of appropriate safety plan	To be completed within 12 days from conclusion of Step 1	Background checks, completion of risk assessment and preparation of DMF paperwork	To be completed within 12 days from receipt of information
Step 3	Referral to DMF	To be completed within 20 days from conclusion of Step 2	Referral to DMF	To be completed within 20 days from conclusion of Step 2
Disclosure to be completed within 10 days from conclusion of step 3				

Step 1 - Initial Contact

Receipt of application and contact with applicant

7.2 At this stage, information should be given to the applicant i.e. a potential victim (hereafter known as 'A') or an interested third party who has some form of contact with 'A' (hereafter known as 'C') advising them of the timescales associated with the process. **NB:** This explanatory information, provided at this stage, is not to

[5] Timescales will be adhered to as far as is practicable.

be confused with who will be eligible to receive disclosure information - any disclosure that may follow should be made to 'A', even if the applicant is 'C', unless there are reasons to do otherwise. This is explained later in the guidance.

7.3 For the purpose of this entry route to the scheme, the trigger that may lead to disclosure occurs when 'A' or 'C' makes a **direct application** to police for information about any known violent or abusive behaviour of a current partner or an ex-partner (hereafter known as 'B').

7.4 If a person makes an enquiry for information to a partner agency rather than PSNI, then normal procedures adopted by the partner agency for handling this type of request should apply. However, if 'A' or 'C' makes it known that they are making an enquiry under the scheme, then they should be referred to PSNI. A partner agency may facilitate contact with the police, if it is appropriate.

7.5 Under **'**Right to Ask', applications can be made by 'A' or 'C' by one of the following means:

- Completing an application form available on the PSNI website at https://www.psni.police.uk/crime/domestic-abuse/dvads/ or via the nidirect website (www.nidirect.gov.uk/see-the-signs);
- Attending a police station in person (you will find a list of all PSNI stations that have public access at www.psni.police.uk);
- Contacting PSNI via 101 (who will direct the individual to make a written application at a police station enquiry office, or to the PSNI website, where they can complete and submit an application form online).

7.6 It is anticipated that the majority of applications by 'A' or 'C' will be made via written application. However, where front-line police officers or a member of police staff (e.g. Station Duty Officer) receive an enquiry during the course of their normal duties, they should advise the individual concerned that a written application should be made to the scheme at a police station, or by completing an application form online. If 'A' or 'C' attends at a police station, they must be afforded the opportunity to make their application in private.

7.7 If at any stage during the initial contact PSNI believe that 'A' or 'C**'** is alleging a crime i.e. a specific incidence of a violent or abusive act, rather than asking for information about a person's previous violent or abusive offending, then PSNI must pursue the crime report under normal criminal investigation procedures. However, it is possible for the process leading to a disclosure under this scheme to run in parallel with a criminal investigation triggered by the allegation of a crime.

7.8 As mentioned, **any disclosure that may follow should be provided to 'A'**, even where 'C' has competently made an application for disclosure. That said, there may be occasions when disclosure to 'A' may not be considered the best approach.

7.9 For example, there may be occasions when ‘A’ is the most appropriate person to receive the disclosure, but for reasons of incapacity, may be unable to fully understand the disclosure information and the potential risks it holds. In such a case, it may be appropriate to identify the person best placed to safeguard ‘A’ and receive disclosure, such as a parent, support work or social worker. They will advise ‘A’ appropriately.

7.10 Following receipt of an application, the applicant (‘A’ or ‘C’) should be contacted by a PPB officer or an associated staff member, to acknowledge the application and ascertain any immediate concerns or issues that may exist in terms of risk. (A safe means of contact will have been recorded on the application form submitted to PSNI).

7.11 The applicant should be informed during this initial contact that a face-to-face meeting should take place within the next 12 days. A suitable date, time and venue should be arranged.

7.12 It is vital that a safe means of communication is further agreed with ‘A’ or ‘C’ where a suitable meeting place, means and timing of communication is determined by them. This is critical to safeguarding the person at possible risk.

7.13 At the outset applicants must be advised of the following:

- a disclosure will only be made to the person (s) best placed to safeguard ‘A’ from harm. This might include a family member or a social worker, for example. This will normally be ‘A’, unless there is a compelling reason not to disclose to ‘A’ e.g. a particular vulnerability has been identifed;

- an overview of the scheme and the timescales for each stage of the process - initial checks will be completed as soon as is practicable, to assess whether the disclosure application should be progressed, and whether there is an immediate or imminent risk of harm to ‘A’ from ‘B’, particularly regarding Articles 2 and 3 ECHR. The person should be provided with a DVADS explanatory leaflet;

- should a decision be made to progress the disclosure application further, the application will be considered by PPB;

- at the face-to-face meeting, ‘A’ or ‘C’ will be required to provide photographic proof of identity and, if the applicant is ‘C’, proof of their relationship with ‘A’, such as text messages or photographs showing evidence of the relationship;

- PSNI will aim to complete the full disclosure enquiry within **45 days**, but there may be extenuating circumstances that require extra time. ‘A’ or ‘C’ will be informed if this is the case;

- If there are risks to ‘A’ identified at any stage, then immediate safeguarding action will be taken to include a robust safety plan. Should a decision be made to disclose to ‘A’, this will be accompanied by a robust safety plan tailored to meet the needs of ‘A’;

- the scheme does not replace existing procedures that are currently in place for subject access of Freedom of Information requests and the Disclosure Barring Service; and

- Should there be any change in their circumstances that may increase risk or impact on safety, they should contact PSNI.

Information checks following initial contact

7.14 Following initial contact with the applicant, minimum information checks should be undertaken to build an initial picture of ‘A’, ‘B’ (and ‘C’, if applicable). This is also to assess whether the application should be progressed. This process will enable officers to check whether ‘B’ poses any immediate risk to ‘A’ or ‘C’. The minimum police checks at this stage are carried out via:

- NICHE;
- Police National Computer (PNC);
- Criminal Record Viewer (CRV);
- Police National Database (PND); and
- ViSOR.

7.15 The information being checked for by PPB involves whether there is any information on systems to demonstrate ‘B’ has a history of violence or abuse which would pose a risk to the potential victim:

- ‘B’ has convictions for an offence related to domestic abuse;
- There is other information (including intelligence) known about the previous violent or abusive behaviour of ‘B’, which may include:
    - Cases not proceeded with; and/or
    - Intelligence concerning violent or abusive offences; and/or
    - Previous concerning behaviour towards former partners – this may include a pattern of behaviours where ‘B’ has exercised coercive control over those partners and information relating to relevant spent conviction/s ; and/or
    - Any other convictions that may be of concern and could be linked to elements of coercive control or display patterns of potentially violent or abusive behaviour.

7.16 As regards checks on ‘A’ or ‘C’, PPB will want to check whether there is any information that may impact on consideration of the application.

7.17 This stage should be completed within **3 days** of the application being received.

7.18 **No disclosure to the applicant should be given by the officer at this stage.**

Decision on whether to progress disclosure application

7.19 The information gathered via the initial contact with the applicant, and the minimum checks, form both the initial risk assessment on ‘A’, and the basis of a decision on whether or not to progress the disclosure application. It will be for an officer of the rank of sergeant or above to review the information and make the decision on whether to progress the disclosure application following the initial checks. In the event of a decision not to progress, then the rationale should be recorded, as should any other action which is instructed.

7.20 In accordance with PSNI procedures, it will be for PPB to determine:

a. whether or not to progress the disclosure application following the completion of initial checks;

b. determine how ‘A’ or ‘C’ will be contacted to progress the disclosure application – as already highlighted, it is vital that, during the initial contact, a safe means of communication is agreed with ‘A’ or ‘C’: a meeting location; means of future communication; and timing of communication that is suitable to them. This is critical to safeguarding ‘A’.

7.21 From the steps outlined above, if it is identified there is an immediate/imminent risk of harm to ‘A’, **action must be taken immediately** to safeguard those at risk, in line with Articles 2 and 3 ECHR.

<u>Step 2 - Face-to-face meeting and risk assessment</u>

7.22 Where an application is to progress, details of the application (not the application form itself) should be shared with other partners, where relevant, as soon as possible after step 1, so that background checks can be carried out on ‘B’ (and ‘A’ and ‘C’ if applicable). Established partner agencies include:

- Probation Board for Northern Ireland;
- MARAC;
- Relevant domestic violence and abuse support services if known;
- Any other relevant partner agency that can provide information to inform the risk assessment if known.

7.23 Partners should provide feedback as regards any relevant information within three working days of receipt of the request from PSNI, for inclusion in the referral to DMF.

7.24 If police decide that a disclosure application should progress, the applicant must be invited to a face-to-face meeting. This is to help:

- ensure that the request is genuine and not malicious;
- establish further details about the application in order to further assess risk, and to inform a decision around disclosure; and
- provide safety information and advice to safeguard 'A'.

7.25 The face-to-face meeting should take place as soon as practicable and, in any event, no later than 12 days after the initial contact.

7.26 At the outset, police will inform the person that should they disclose any alleged crime PSNI is duty bound to initiate an investigation into this alleged crime if it has not previously been reported to police.

7.27 It is possible for procedures leading to a disclosure under the scheme to run in parallel with any criminal investigation. All contact with the applicant will be recorded on the application form and the face-to-face meeting must take place within a safe environment for the applicant.

At the face-to-face meeting

7.28 Before progressing enquiries on the application, the PPB officer must:

- warn 'A' or 'C' that if they wilfully or maliciously provide false information to PSNI in order to try to obtain a disclosure they are not entitled to, that they may risk prosecution e.g. if they have provided false details in an attempt to make a malicious application, they may be prosecuted under section 5(3) of the Criminal Law Act (NI) 1967[6]. If this is suspected, the evidence to support such a suspicion must be fully documented;

- warn 'A' or 'C' that if they disclose evidence of an offence whilst registering a concern, it may not be possible to maintain their confidentiality;

[6] section 5(3) of the Criminal Law Act (NI) 1967 provides that "where a person causes any wasteful employment of the police by knowingly making to any person a false report or statement tending to show that an offence has been committed, whether by himself or by another person, or to give rise to apprehension for the safety of any persons or property, or tending to show that he has information material to any police inquiry, he shall be liable on summary conviction to imprisonment for not more than six months or to a fine of not more [level 4 on the standard scale] or to both".

- warn ‘A’ or ‘C’ that information disclosed by PSNI must only be used for the purpose for which it has been shared i.e. to safeguard ‘A’;

- assure ‘A’ or ‘C’ that the application will be dealt with confidentially. There should, however, be a caveat placed on this – that confidentiality can only be guaranteed pending the outcome of the risk assessment process. If a resultant disclosure is to be made to ‘A’ or ‘C’, PSNI must consider whether ‘B’ should be informed. If such a disclosure would increase the risk to ‘A’, or any other person, ‘A’ or ‘C’ should be informed that it will not be made;

- where ‘A’ makes the request, ensure they are aware of support available within the DVADS process; and

- ask ‘A’ or ‘C’ for photographic proof of identity, which will include:
    - passport;
    - driving licence;
    - other trusted form of photo identification.

7.29 Whilst photo identification (along with confirmation of date of birth and address) is required, it is accepted that some of the vulnerable individuals who make applications may not have the above forms of identification. In these cases it may be possible to refer to another agency to confirm the individual’s identity (e.g. health visitor, social worker).

7.30 A disclosure cannot be made to ‘A’ or ‘C’ without verification of identity, or if the applicant chooses to remain anonymous. However, if either of these two eventualities arise, checks should still be made on the information given about ‘B’ and, if concerns are identified, then the application should be treated as an intelligence submission which may be used to inform safeguarding measures for ‘A’, under ‘Power to Tell’.

Information to be obtained during the face-to-face meeting

7.31 Police should confirm the following information from ‘A’ or ‘C’ which will have been obtained at initial application stage:

- name including any other names used;
- date of birth;
- place of birth;
- address

7.32 Further details must also be obtained from the applicant to confirm the reliability of the application:

- reason for contact;
- history of relationship between ‘A’ and ‘B’.

7.33 ‘A’ or ‘C’ should be told that the person to whom the disclosure is made will be asked to sign an undertaking stating they agree that the information is confidential and that they will not disclose this information further. A warning must be given that legal proceedings could result if this confidentiality is breached and that it may also be a breach of section 55 of the Data Protection Act 1998 for a person to knowingly or recklessly obtain or disclose personal data without the consent of the data controller (i.e. the agency holding the information that will be disclosed, which in most cases will be PSNI).This should be explained to the person and their signature obtained on this undertaking.

7.34 If the person is not willing to sign the undertaking, the PPB officer will record this and inform DMF. The forum will then need to consider whether disclosure should still take place. The outcome should be recorded and considered in the subsequent risk assessment and decision making process.

7.35 Following the face-to-face meeting, the PPB officer should carry out a full risk assessment.

7.36 **Where the applicant is ‘A’**, the Domestic Abuse, Stalking and Harassment and Honour Based (DASH) form should be completed. Where stalking is identified, the S-DASH risk assessment should also be completed. Completion of the DASH form is vital to establish an appropriate safety plan for ‘A’. It is, therefore, important that ‘A’ understands the purpose of DASH is to establish the level of risk and to consider appropriate victim safety measures.

7.37 Officers completing DASH must bear in mind that ‘A’ may be unaware that they are a victim, or that police have a duty to investigate and raise a crime report. The officer must clearly state at the outset of the meeting that should a crime be disclosed it **must** be recorded and an investigation will be commenced if the crime had not previously been reported to police. Should the victim disclose a crime or offence, then the following process should be adopted:

- officers will complete the DASH if already commenced;
- officers must afford the victim the opportunity to report the incident and make a statement.

7.38 During the face-to-face meeting and completion of DASH, the applicant should be offered an information leaflet explaining DVADS. It may not be appropriate to provide information leaflets to the applicant, where there is a risk that this information could get into the wrong hands. A victim safety plan should also be discussed, if deemed appropriate.

7.39 It should be noted that DASH is very much a dynamic risk assessment tool and should be reconsidered in light of additional information provided by ‘A’ or ‘C’,

partner agencies and checks on PSNI systems. The research and checks should fill any gaps in information and this stage should help ensure all available information known to PSNI on the individuals concerned with the enquiry has been established.

7.40 Checks will also be completed with other agencies and partners, where applicable.

7.41 **Where the applicant is 'C'**, a DASH form should not be completed at this stage, given that there is no direct contact with the person at risk. (A risk assessment will be carried out on contact with the potential victim at a later stage). Instead, the PPB officer should consider whether, 'concern' or 'no concern' exists and whether, a decision to disclose information should be referred to DMF.

7.42 This step should be completed within 20 days from the completion of step 2.

Power to Tell

7.43 The timescale for this aspect of the scheme is 42 days (see timescale table detailed at paragraph 7.2 above).
Indirect information received by PSNI

7.44 Under 'Power to Tell', the trigger which may lead to a disclosure under DVADS is where PSNI receive indirect information that may impact on the safety of an individual and which has not been conveyed via the 'Right to Ask'.

7.45 Indirect information is likely to be information received by PSNI from intelligence-gathering arising from the following activities:

- an investigation into a crime where, as part of that investigation, PSNI has reason to believe that 'A' may be at risk of harm from 'B';
- information on alleged offending by 'B' that is received from;
    - partner agencies (statutory and/or third sector) as part of routine information sharing at MARAC;
    - intelligence sources;
    - either 'A' or 'B' coming into contact with PSNI as part of their routine operational duties.

7.46 Following receipt of the indirect information, intelligence checks should be undertaken by PPB to build an initial picture on 'A' and 'B'. This will help inform officers whether 'B' poses any immediate risk to 'A' and also, to assess whether the matter should be progressed.

7.47 **If it is identified that there is an immediate/imminent risk of harm to 'A' or any other person, action must be taken immediately to safeguard those at risk, in line with Articles 2 and 3 ECHR.**

7.48 The minimum police checks at this stage are:

- NICHE;
- Police National Computer (PNC);
- Criminal Record Viewer (CRV);
- Police National Database (PND);
- ViSOR

7.49 Similar to 'Right to Ask', the information to be checked under 'Power to Tell' involves whether there is any information to demonstrate 'B' has a history which would pose a risk to the potential victim:

- 'B' has convictions for an offence related to domestic abuse;
- There is other information (including intelligence) known about the previous violent or abusive behaviour of 'B', which may include:
    - Cases not proceeded with; and/or
    - Intelligence concerning violent abusive offences; and/or
    - Previous concerning behaviour towards former partners – this may include a pattern of behaviours where 'B' has exercised coercive control over those partners and information relating to relevant spent conviction/s ; and/or
    - Any other convictions that may be of concern and could be linked to elements of coercive control or display patterns of potentially abusive behaviour.

7.50 Processes under the National Intelligence Model should also be used to determine, as far as possible, the veracity of the indirect information received.

7.51 To ensure that the safeguarding response is proportionate and in line with the risks identified, PPB may prioritise which potential disclosures receive a full risk assessment. To assist in the process, consideration should be given to whether 'A' is:

- judged to be at 'high', 'medium' or 'standard' risk of harm from 'B';
- associated with a serial perpetrator of domestic violence or abuse.

7.52 On the basis of its findings from the completion of intelligence checks, PSNI may make the decision not to progress the disclosure. This decision should be recorded appropriately. It will be for an officer of the rank of Sergeant or above to review the information and make the decision on whether to progress the disclosure. In the event the decision is not to progress, then the rationale should be recorded, as should any other action which is instructed.

7.53 This step should be completed within three days of the application being received.

Step 3: PPB referral to the multi-agency forum - DMF

7.54 At this point in the DVADS process, it is envisaged that, under either 'Right to Ask' or 'Power to Tell', sufficient information should have been gathered and checked to determine whether a credible risk of harm to 'A' in the form of previous domestic violence and abuse behaviour from 'B' exists. This will include checks made with partner agencies for any information they may hold on 'A', 'B' (or 'C', if relevant).

7.55 While it will be for DMF to recommend whether a disclosure should be made by PSNI, police should provide its categorisation of the disclosure as either a 'concern' or 'no concern'. DMF should consider this categorisation. The matter should be referred to the forum within 20 days from conclusion of step 2.

Categorising a 'concern' or 'no concern'

7.56 A **'concern'** occurs if 'A' is at risk of harm from 'B', based on a balanced profile of 'B' that takes into account the following factors:

- 'B' has convictions for an offence related to domestic abuse;

- There is other information (including intelligence) known about the previous violent or abusive behaviour of 'B' which may include:
    - Cases not proceeded with; and/or
    - Intelligence concerning violent or abusive offences; and/or
    - Previous concerning behaviour towards previous partners. This may include a pattern of behaviours where 'B' has exercised coercive control over previous partners, or information relating to relevant spent conviction/s; and/or
    - Any other convictions that may be of concern and could be linked to elements of coercive control or display patterns of potentially abusive behaviour.

- There is concerning behaviour by 'B' demonstrated towards 'A'. This may include a pattern of behaviours that indicates 'B' is exercising coercive control over 'A'.

7.57 Where police consider the disclosure of relevant spent convictions to be applicable under the scheme, it is important that disclosure is reasonable and proportionate. PSNI will want to take account of the age of the spent conviction during the decision making process. Legal advice should be sought where necessary. Where such disclosure is lawful, the Rehabilitation of Offenders (Exceptions) Order (Northern Ireland) 1979 provides a legal exemption from prosecution for the disclosure.

7.58 If there is deemed to be a 'concern', PPB must consider if representations should be sought from 'B' to ensure that officers have all necessary information to make a decision in relation to disclosure. As part of this consideration, PPB must also consider whether there are good reasons not to seek representation, such as the need to disclose information in an emergency or seeking that representation may put 'A' at risk.

7.59 Under 'Right to Ask' a '**no concern**' does not generally reach DMF stage. PSNI will have checked its systems for information, and it will have consulted with its partner agencies.

7.60 A **'no concern'** that reaches DMF stage mainly applies to 'Power to Tell' where:

- PPB has not found any convictions for an offence related to domestic violence or abuse;
- PPB has not found any other intelligence that indicates that 'B's behaviour may cause harm to 'A'; or where
- there is insufficient intelligence or information to register a concern;
- there are no other convictions of concern that could be linked to elements of coercive control or display patterns of potentially abusive or violent behaviour.

And

- where PPB has not had the opportunity to consult with partner agencies to gather further information (as would be the case under 'Right to Ask'); and
- where referral to DMF would provide it with that opportunity, and allow the case to be considered and re-assessed.

7.61 Once PSNI has determined whether the initial trigger can be recorded as a 'concern' or 'no concern', the case must be referred to DMF for consideration at its next meeting (bearing in mind the timescales provided for in this guidance).

7.62 It will be for DMF to make the final recommendation on whether the trigger is a 'concern' or 'no concern' based on the information gathered by PPB and whether to recommend that disclosure should be made or not. **PSNI will ultimately make the decision on whether or not disclosure should take place.**

7.63 **If it is identified there is immediate/imminent risk of harm to 'A' or any other person, then action must be taken immediately by PSNI to safeguard those at risk, in line with Articles 2 and 3 ECHR.**

The Decision Making Forum (DMF)

7.64 DMF is operated under the auspices of the current MARAC framework, as well as the existing procedures governing MARAC convention and operation. DMF must, therefore, adhere to the existing MARAC Information Sharing Agreement and Operating Protocol. DMF will form a specific meeting, following on from the main MARAC meeting. Typically these will be convened once a month.

7.65 DMF membership will comprise the same representation as is included for MARAC, so as to enable risk to be fully considered and assessed and to help safeguard 'A' and their children. The minimum number of bodies constituting DMF should be no less than three, to include PSNI which leads in this area and must be included on all occasions. Groups that make up DMF need to be registered data controllers, and have appropriate data security policies and procedures in place.

7.66 DMF is chaired by the relevant PPB sergeant for the area (as is the case for MARAC). The PPB Sergeant, following the DMF meeting and having regard for the determination reached by the forum, will refer their decision on disclosure (including decision not to disclose) to the relevant PPB Inspector for approval.

7.67 DMF should consider the referral no later than 20 days after the categorisation of the 'concern' or 'no concern' has been made by PSNI.

7.68 Where it has been identified that there is an imminent or immediate risk of harm to 'A', or any other person, PSNI must take immediate action to safeguard those at risk, in line with Articles 2 and 3 ECHR.

7.69 In the event that an urgent disclosure is considered necessary, and is made by PPB, referral to DMF will be made retrospectively, for its information and for completeness of the process.

DMF principles

7.70 DMF must consider certain decision making principles when making a disclosure recommendation to PSNI. (See Annex E, which outlines the Data Protection Act 1998 General Principles.) There are **three principles** that DMF must take into account:

Principle 1: Three-stage disclosure test (lawfulness, necessity and proportionality)

7.71 As already mentioned, PSNI has the power to disclose information about an individual, where it is necessary to do so to protect another individual from harm. The following three stage test should be satisfied before a decision to disclose is made:

i. that DMF will make a recommendation to PSNI to disclose information about 'B' to 'A' or 'C'. As PSNI is relying on its common law and statutory power to disclose, it must be shown that it is reasonable to conclude that disclosure is necessary to protect the public, or particular sections of the public, from crime. This would make the disclosure **lawful**;

ii. PSNI will be required to conclude that disclosure is **necessary** to protect 'A' from harm or being a victim of crime; and

iii. any disclosure that interferes with 'B's rights - under Article 6 and Article 8 of the European Convention on Human Rights (ECHR), the Data Protection Act 1998 and the forthcoming General Data Protection Regulation - must be **proportionate**. The principles of proportionality remain essential to decision making, and will only be undertaken after all factors have been considered and the threat carefully assessed. This will include, among other matters, considering the possible consequences for 'B' if information is disclosed about the nature and extent of the risks that 'B' poses to 'A'. There must be a balance of the rights of 'B' against the need to prevent harm and crime and all decisions in this regard must be documented. This stage of the test involves considering:

    a. whether 'B' should be asked if they wish to make representation, so as to ensure PSNI has all the necessary information at its disposal to conduct the Article 8 balancing exercise. This should include considering any risk identified to a previous victim or a third party making an application, which may arise as a consequence of the scheme's process, to help ensure those persons are also protected, as may be required; and

    b. the extent of the information which needs to be disclosed – e.g. it may not be necessary to tell the applicant the precise details of the offence for the applicant to take steps to protect 'A'.

7.72 There may be concerns that relate to 'B's current behaviour towards 'A' within the disclosure application e.g. abusive or threatening behaviour. In this case, even though there is no recorded information held by PSNI or other agencies to disclose to the applicant, the applicant may still be contacted to talk about the decision-making forum's concerns over 'B's current behaviour.

7.73 This discussion should cover the steps the applicant should take in relation to these concerns to safeguard 'A' from the risk of harm posed by 'B'. The forum will consider what safeguarding measures could be introduced to initially support 'A' and determine the action each agency could offer to ensure that the safety plan remains victim-centred.

Principle 2: Data Protection Act 1998

7.74 The type of information about 'B' which is likely to be under consideration in terms of DVADS is both 'personal data' and 'sensitive personal data' in terms of the Data Protection Act.

7.75 DMF must be satisfied that disclosure is in accordance with the eight principles of the Act (see Annex E for details of these principles and guidance on how they can be practically applied). The first principle is not relevant if section 29 of the Act applies, but one of the conditions in Schedule 2 and one of the conditions in Schedule 3 must still be met.

7.76 Generally speaking, so long as there is adherence to this guidance, then sharing of such information or any disclosure of same (or some of it) will accord with the relevant provisions of the Act.

Principle 3: Informing 'B' of the disclosure

7.77 Consideration must also be given as to whether 'B' should be told that information about them may be disclosed to the applicant. Such a decision must be based on an assessment of risk of harm to 'A', if 'B' were to be informed.

7.78 Due consideration must be given to whether the disclosure to 'B' would have the potential to escalate the risk of harm to 'A'. Similarly, any risk to a previous victim or a third party making an application, which may arise as a consequence of the scheme's process, should also be considered. If this were to be the case, no disclosure must be given to 'B'.

7.79 In the event that 'B' is to be informed that a disclosure is to be made to the applicant, then 'B' should be informed in person and given information about the scheme and the implications for them.

Disclosure of Information

7.80 If DMF makes a recommendation to PSNI to disclose information because it judges that there is a risk of harm to 'A' that warrants a disclosure, then it should consider the following points:

- what will be disclosed?
    - DMF will consider and recommend the specific wording of a proposed disclosure that contains sufficient information to allow the recipient to make an informed choice with regard to their relationship with 'B'. The disclosure must be accompanied by a robust safety plan tailored to the

needs of ‘A’ and based on all relevant information, which identifies the service provision and the agency leads who will deliver on-going support to ‘A’. In agreeing the wording of a disclosure, DMF must ensure that the information contained in any disclosure must also not prejudice any current or potential future investigations and prosecutions of ‘B’, in which ‘A’ may be a victim or witness. For example, DMF must consider the impact of disclosing details of ‘B’s Modus Operandi with previous victims. Additionally, consideration must also be given to any risk posed to a previous victim or a third party making an application, as a direct consequence of the scheme’s process, to help ensure those persons are also protected, as may be required.

- to whom should the disclosure be made?

    - The disclosure should be provided to the person(s) best placed to safeguard ‘A’. Whilst it is envisaged that the majority of disclosures will be made to ‘A’, it may not be appropriate to do so in all instances. The judgement of who to disclose to will be determined by DMF following the information gathered as part of the DVADS process and subsequent risk assessments.

- how the disclosure should be made?

    - The disclosure will be delivered by PPB, however DMF will consider whether joint-agency delivery is best, based on the information at hand. It is good practice to consider a joint-agency approach to the disclosure provision.

    - The disclosure will be made in person. In line with safeguarding procedures, it is essential that the disclosure takes place at a safe time and location to meet the specific needs of ‘A’.

    - The inclusion of support at the disclosure meeting, which is considered best practice. A joint VSNI and Women’s Aid arrangement has been agreed whereby contact should be made by PPB to enable inclusion of a support worker if available to attend the disclosure meeting (including non-disclosure). However, ‘A’ must provide consent for a support worker to be present during this meeting. **Note**: Should there be third party attendance at the disclosure (i.e. support worker, family member or friend known to ‘A’), then the third party must also be provided with the same form of words around warning and information sharing and they should be asked to also sign the undertaking form.

7.81 If disclosure is made, then the person receiving the disclosure must be advised of the following:

- that the disclosure must only be used for the purpose for which it has been shared i.e. in order to safeguard 'A';

- the person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and that they may only share the information further, with due regard for others' right to privacy and right to fair trial, in order to safeguard themselves;

- the person to whom the disclosure is made will be asked to inform PSNI of any intention to share the information and with whom they intend to share it with;

- a warning should be given that legal proceedings could result if this confidentiality is breached. This should be explained to the person and they must sign the undertaking.

7.82 If the person is not willing to sign the undertaking, PSNI will need to consider if disclosure should still take place. The outcome should be recorded and considered in the risk assessment, decision-making process and safety plan.

7.83 At **no time** will written correspondence concerning the specifics of the disclosure be sent to, or left with, the applicant in relation to the disclosure of information. This would present a potential risk to intelligence sources, victims and perpetrators should such written information fall into the wrong hands.

7.84 What the applicant is told at disclosure should be recorded verbatim on the form and signed by them. **It must not be given to the applicant under any circumstances and will be retained by PSNI's PPB.** Officers must ensure that the applicant fully understands the information being explained to them.

7.85 The person to whom the disclosure is made should be given information to assist them in safeguarding 'A'.

*Decision made **not** to disclose information*

7.86 If a decision is made not to disclose information because it is judged that there is a no risk of harm to 'A' that warrants a disclosure, then these actions should be followed by DMF:

i. if the decision not to disclose has been made following **'Power to Tell'**, then the decision not to disclose plus the rationale should be recorded. Recording the decision in this way may inform future disclosure considerations made on 'B'.

ii. if the decision not to disclose has been made following **'Right to Ask'**, then the following steps should be taken:

a) it is highly recommended that the applicant should be told in person, via a safe telephone number if appropriate, as any written correspondence has the potential to put 'A' at more risk. The applicant should be told that there is no information to disclose on the basis of the information/details provided by the applicant and the result of checks made on these details;

b) However, it is important that the applicant is told that the lack of information to disclose does not mean that there is no risk of harm to 'A' and that they should remain vigilant and report any future concerns. This contact also presents an opportunity to provide safeguarding information and signposting to relevant support services;

c) the applicant should be given information to help safeguard 'A' in the future, but at no time should this information contain written correspondence concerning the specifics of the disclosure consideration. There would be a potential risk of harm to 'A' should such written information be obtained by a third party and/or 'B'.

iii. 'B' will not be notified, where no disclosure is made to the applicant.

Maintaining a record of the disclosure scheme

7.87 At the closure of every case (whatever the outcome, and at any stage in the process) a final report must be submitted onto PSNI intelligence systems to record the request/information received, outcomes and details of all parties involved. This should serve as a piece of valuable intelligence, (which will be retrievable to all police forces via the PND system). It would allow any patterns where 'B' has many disclosure requests made against them to be identified to help safeguard 'A'.

7.88 Any decisions made as a result of this scheme must be human rights compliant. They must be recorded fully and in a format that would stand scrutiny of any formal review including judicial review.

7.89 It is also crucial that any relevant information coming to light as part of this process is shared, as appropriate, with all relevant agencies, in accordance with the principles of information sharing and disclosure, as articulated in this guidance document.

Keeping People Safe

OFFICIAL [PUBLIC]

DOMESTIC VIOLENCE AND ABUSE DISCLOSURE SCHEME

'RIGHT TO ASK/'POWER TO TELL'

Application Form

***Sections with an asterisk are mandatory fields and must be completed.**

OFFICIAL USE ONLY	
NICHE Occurrence No:	Decision Making Forum Case Number:
Date Application received:	**Officer/Staff Completing:** Name: Rank: Police No:/Staff No: How was contact made? Persons at Station Email
Step 1 date commenced: Step 1 date completed:	**Officer/Staff Completing:** Name: Rank: Police No/Staff No: How was contact made?
Step 2 date commenced: Step 2 date completed:	**Officer/Staff Completing:** Name: Rank: Police No/Staff No: How was contact made?
Step 3 date commenced: Step 3 date completed:	**Officer/Staff Completing:** Name: Rank: Police No/Staff No: How was contact made?

I understand that my copleting and submitting this application the information provided in this form will be processed and used by Police to conduct checks so that individuals who may be at risk can be identified. Information may be shared with partner agencies in order to do this within the remit of the scheme. In circumstances where child protection matters are identified the information will be passed to the relevant Social Services Trust in written form as soon as possible.

SECTION 1 - DETAILS OF THE APPLICANT (FULL NAME REQUIRED)	
Surname:*	Forename(s):*
DOB:*	Place of Birth:*
Address (in full - including postcode):*	Ethnic Origin:*
Gender:*	Occupation:*
Preferred method of Contact:*	Preferred time of Contact:*
Preferred Contact Number:*	Preferred Language:*

SECTION 2 - DETAILS OF PERSON AT RISK - IF DIFFERENT FROM APPLICANT (FULL NAME REQUIRED)	
Surname:*	Forename(s):*
DOB:*	Place of Birth (if known):*
Address (in full)*	Ethnic Origin:*
Gender:*	Occupation:
Preferred method of Contact:	Preferred time of Contact:
Preferred Contact Number:	Preferred Language:*

It is vital that during this initial contact, a safe means of communication is agreed with the applicant where the place, means and timing is determined by the applicant. **This is critical to safeguarding of the applicant.**

Safe contact details:

Name:* _____

Telephone Number:* _____

SECTION 3 - DETAILS OF THE SUBJECT (FULL NAME REQUIRED) - Who do you want to ask information about? (The more details police have concerning the subject, the easier it will be to carry out necessary police checks) **NOTE:** If DOB is not provided Police may not be able to carry out the appropriate checks.	
Surname:*	Forename(s):*
DOB:* (if unknown please include an approximate age)	Place of Birth (if known):
Address (in full - including postcode if possible):	Ethnic Origin:
Gender:*	Occupation:
Previous Addresses (if possible)	Employer and Place of Work:
Relationship to person at risk:*	
Contact Number (if known)	
Additional information/other names/alias names:	

SECTION 4 - DETAILS OF CHILD AT ADDRESS OR WITHIN THE RELATIONSHIP **Are there any children at the address or within the relationship (including) children who live elsewhere)** **Yes** ☐ **No** ☐ **If no please proceed to section 5** **If yes please provide details:**	
CHILD 1	
Surname:*	Forename(s):*
DOB:*	Place of Birth:
Address (in full - including postcode):*	Ethnic Origin:*
Gender:*	

CHILD 2	
Surname:	Forename(s):
DOB:	Place of Birth:
Address (in full - including postcode):	Ethnic Origin:
Gender:	

CHILD 3	
Surname:	Forename(s):
DOB:	Place of Birth:
Address (in full - including postcode):	Ethnic Origin:
Gender:	

Please enter details of any additional children below, using the previous layout:

SECTION 5 - DETAILS OF REGISTERED INTEREST - Why are you concerned?
What has prompted you to register an interest in the subject? *Please provide all necessary details:*
Is it information you are aware of or concerned about? **Yes** ☐ **No** ☐ *If yes please provide all necessary details:*

Is it the person at risk's behaviour/information - Has the person at risk given you information or behaved in a way that has raised concerns? **Yes** ☐ **No** ☐
If yes please provide all necessary details:

Is it the Subject's behaviour/own observations - Has the subject behaved in a way or have you observed the subject in a way that raises concerns? **Yes** ☐ **No** ☐
If yes please provide all necessary details:

Is it Something Else? - See explanatory note **Yes** ☐ **No** ☐
If yes please provide all necessary details:

Any other relevant information? Please see explanatory note
Please provide all necessary details:

SECTION 6 - ELEMENTS OF RISK - SAFETY QUESTIONS

Does the subject know you are making this application?* YES ☐ NO ☐

Are you concerned about the subject know that you are making this application?* YES ☐ NO ☐

If yes, please provide all necessary details

If you are applying about someone else's partner does that person know that you are making this application?* YES ☐ NO ☐

Do you think there is an immediate risk that Police should act quickly on?* YES ☐ NO ☐

If yes please provide all necessary details

NB: If you believe there is an immediate risk, you should also report this to police immediately via telephone on 999 (in emergencies) or 101 (for non-emergencies) or by reporting personally at a police station.

Is there anything else you feel Police should know? (Please inform us about any other risks, concerns or comments you might have).

INFORMATION TO BE READ BY THE APPLICANT OR TO READ TO THE APPLICANT BY THE COMPLETING OFFICER/STAFF MEMBER:*

The Domestic Violence and Abuse Disclosure Scheme does not replace existing procedures that are currently in place for the Disclosure and Barring Service. Subject Access or Freedom of Information requests, nor does it replace existing Safeguarding Adult procedures. Where an enquiry is made that is unsuitable for the disclosure scheme, Safeguarding Adult procedures may be taken.

Disclosure will only be given to the person at risk and/or the person who is in the best position to safeguard the person at risk from harm.

Relevant checks should be completed by POLICE using the information given in this form. The results of these checks will be used to assess whether there is an immediate and imminent risk of harm to the person at risk from the subject.

Should a decision be made to progress the disclosure application further then this will be referred to the PSNI's Public Protection Team to follow up. There will be a face-to-face discussion with the applicant by a specially trained officer. This should take place no later than 12 days after the initial contact. You are advised that a credible proof of identity will be required at this stage (preferably photo ID such as a passport or driving licence). From this the necessary checks and risk assessments MUST be completed which will then be discussed at the Decision Making Forum before any disclosure can be made. Other than in exceptional circumstances, applications for disclosure should be completed within 45 days of initial contact.

If any immediate risks are identified at any stage, then immediate safeguarding action will be taken, including a rebust safety plan delivered by PSNI and partners.

Do you consider yourself to be at risk from the subject of this enquiry?* **YES** ☐ **NO** ☐

If yes, follow the appropriate action to address any concerns and identified risks regarding domestic abuse and personal security. For further information please consult PSNI Domestic abuse information pages on the PSNI external website www.psni.police.uk

PLEASE NOTE:

I understand that by submitting this application the information provided in this form will be processed and used by Police to conduct checks so that individuals who may be at risk can be identified. Information may be shared with partner agencies in order to do this within the remit of this scheme.

IN CIRCUMSTANCES WHERE CHILD PROTECTION CONCERNS ARE IDENTIFIED THE INFORMATION WILL BE PASSED TO THE RELEVANT SOCIAL SERVICES TRUST.

By signing below:

- I understand that if I have wilfully given false or malicious information to the obtain information about another person, I may be liable to criminal proceedings.
- I understand that, should I receive a subsequent disclosure regarding the person I have enquired about, this will be solely for the purpose of keeping myself and/or my child(ren) safe.
- I understand that I must not share this information with any other person.
- If I breach this confidentiality, I understand that I may be liable to legal proceedings depending upon the circumstances.
- I agree that should I receive a disclosure, I will abide by an undertaking to keep this information confidential.

Applicants Name (BLOCK CAPITALS):*	
Signature:*	Date
Officer/Staff completing:*	Date
Service/Staff number*:	

How did you hear about the Disclosure Scheme?

PSNI website	☐	Poster	☐	TV advert	☐
NIdirect website	☐	Word of mouth	☐	Press Advert	☐
Leaflet	☐	Radio Advert	☐	Other	☐

If other, please specify: _____

SECTION 7: DISCLOSURE SCHEME CRITERIA (OFFICIAL USE)

Does the information provided meet the criteria of the Disclosure Scheme: YES ☐ **NO** ☐

Please provide rationale below

Domestic Violence and Abuse Disclosure scheme application - Explanatory Note

Section 1 – Applicant Details

- **Ethnic origin** - This information is necessary so that Police can carry out our checks thoroughly and to identify if there are any special requirements for example religious or cultural considerations.
- **Place of birth** - This information is important as this will identify if further checks will be required for example if a person was born in a different country or in a different Health Trust area.
- **Gender** - This information is important to ensure that our scheme is S75 compliant and that we can ensure that the scheme is open to all members of the community. We can use this information to ascertain if further awareness raising is required for a specific side of the community to ensure inclusion.
- **Occupation** - This information is important as this could identify potential safeguarding actions that are required or other potential risks to other people. If we do not have this information we may not be able to take any action to manage potential risks or to protect people.
- **Preferred method of contact** - This information is necessary because PSNI need to be able to contact you at a safe time and by a safe means so as not to put the you at any unnecessary risk.
- **Preferred time of contact** - This information is important as the PSNI need to be able to contact the you on a safe number this may not necessarily be the applicants own telephone number.
- **Preferred contact number** - This information is important as the PSNI need to be able to contact the you on a safe number this may not necessarily be the applicants own telephone number.
- **Preferred language** - This information is necessary so that PSNI can communicate properly with you and obtained accurate information. This will allow the PSNI to arrange for an interpreter if required.
- **Are you the person at risk?** This information is necessary as it will dictate which section of the form you will be directed to next for completion.

Section 2 – Person who may be at Risk details

- **Place of birth** - This information is important as this will identify if further checks will be required for example if a person was born in a different country or in a different Health Trust area.
- **Ethnic origin** - This information is necessary so that Police can carry out our checks thoroughly and to identify if there are any special requirements for example religious or cultural considerations.
- **Gender** - This information is important to ensure that our scheme is S75 compliant and that we can ensure that the scheme is open to all members of the community. We can use this information to ascertain if further awareness raising is required for a specific side of the community to ensure inclusion.
- **Occupation** - This information is important as this could identify potential safeguarding actions that are required or other potential risks to other people. If we do not have this information we may not be able to take any action to manage potential risks.
- **Preferred method of contact** - This information is necessary because PSNI need to be able to contact the person at risk at a safe time and by a safe means so as not to put the applicant at any unnecessary risk.

- **Preferred contact time** - This information is necessary because PSNI need to be able to contact the person at risk at a safe time and by a safe means so as not to put the person at any unnecessary risk.

- **Preferred contact number** - This information is important as the PSNI need to be able to contact the applicant on a safe number this may not necessarily be the applicants own telephone.

- **Preferred language** - This information is necessary so that PSNI can communicate properly with the applicant and obtained accurate information. This will allow the PSNI to arrange for an interpreter if required.

- **Safe contact details** - This information is important as the PSNI need to be able to contact the applicant on a safe number this may not necessarily be the applicants own telephone number and may be different to the preferred contact number.

- **Safe name** - These are the details Police will use to make contact with you to arrange a meeting and to obtain information. You need to be content that this is a safe means to contact you.

- **Safe telephone number** - This information is important as the PSNI need to be able to contact you on a safe number this may not necessarily be the applicants or person at risks own telephone number. This could be a friend, relative, work number etc but you must be content that this will not put you at any risk. This may be different to the preferred contact number above. This information is important as the PSNI need to be able to contact you on a safe number this may not necessarily be the applicants or person at risks own telephone number. This could be a friend, relative, work number etc but you must be content that this will not put you at any risk. This may be different to the preferred contact number above. This information is used to minimise the risk that the person may be exposed to should the Police need to contact them.

Section 3 – Subjects details (the person you are concerned about)

- **Date of birth** - Police will use this information to check for details of the subject. If a date of birth is not provided we may not be able to check our records. An approximate age would be helpful.

- **Place of birth** - This information is important as this will identify if further checks will be required for example if a person was born in a different country or in a different Health Trust area.

- **Ethnic origin** - This information is necessary so that Police can carry out our checks thoroughly and to identify if there are any special requirements or considerations for example religious or cultural considerations.

- **Gender** - This information is important to ensure that our scheme is S75 compliant and that we can ensure that the scheme is open to all members of the community. We can use this information to ascertain if further awareness raising is required for a specific side of the community to ensure inclusion.

- **Occupation** - This information is important as this could identify potential safeguarding actions that are required or other potential risks to other people. If we do not have this information we may not be able to take any action to manage potential risks.

- Previous address - This information is important as this will identify if further checks will be required for example if a person lived in a different country or in a different Health Trust area or perhaps with another person.

- **Relationship to person at risk** - They must be partners in order to be eligible for this scheme.

- **Contact number** - This number may be used to contact the subject if Police need to speak with them for example if any risk posed to them.

- **Additional information/other names/aliases** - This information will enable Police to accurately check records for any information that may identify risk.

Section 4 – Childrens details

- **Children's details** - These details are necessary to enable police to accurately check records and may identify potential risks or safeguarding actions that would be required. If we do not get these details Police will not be able to accurately assess risk or carry out this function and fulfil their obligations under Child Protection.

- **Date of birth** - Police will use this information to check for details of the children and any risks/ concern that may need acted upon. If a date of birth is not provided we may not be able to check our records. An approximate age would be helpful.

- **Surname** - This may be different from person at risk or subject and could identify other risks/ concerns that Police and other agencies would need to be aware of in order to take appropriate safeguarding actions.

- **Place of birth** - This information is important as this will identify if further checks will be required for example if a person was born in a different country or in a different Health Trust area.

- **Address** - This information will be used to check if there have been any incidents of concern at this address which may give rise to concern for children or person at risk. If identified appropriate safeguarding measures can be considered.

- **Ethnic origin** - This information is necessary so that Police can carry out our checks thoroughly and to identify if there are any special requirements for example religious or cultural considerations.

- **Gender** - This information is important to ensure that our scheme is S75 compliant and that we can ensure that the scheme is open to all members of the community. The information will also be used to accurately identify the person from any records held. We can use this information to ascertain if further awareness raising is required for a specific side of the community or other agencies to ensure inclusion for example schools.

Section 5 – Details of registered interest – Why are you concerned?

- **What has prompted you to register an interest in the subject?**

  Tell us why you are applying to the scheme. Police need to understand why you are concerned. If there are no concerns the application will not qualify for the scheme. 250 word maximum

- **Is it information you are aware of or are concerned about?**

  If you answer yes please provide details as Police need to understand what you find concerning from the information that you have. 100 word limit.

- **Is it the Person at Risk's/behaviour/information - Has the person at risk given you information or behaved in a way that has raised concerns?**

  If you answer yes please provide details as police need to understand what you are concerned about and why this information or type of behaviour has caused you to become concerned. 100 word limit.

- **Is it the Subject's behaviour/own observations - Has the subject behaved in a way or have you observed the subject in a way that raises concerns?**

  If you answer yes please provide details as police need to understand whay you are concerned and explain what information or the type of behaviour has caused you concern and why. 100 word limit.

- **Is it something else?**

  If you answer yes and your concerns have not fitted into any of the previous categories this is your opportunity to explain what it is that has caused you concern and why? for example is it something a child has said? Is it a change in a child's behaviour or reactions, is it based on your own previous experience of the subject etc. 100 word limit.

- **Any other relevant information**

  You may use this section to highlight any risks or concerns that you feel have not been identified anywhere else on the form that could require safeguarding actions or consideration e.g is the subject involved in any voluntary capacity with vulnerable members of the community sporting activity, youth work etc.100 word limit.

Section 6 – Elements of risk – Safety Questions

- **Does the subject know you are making this application?** - This information is used to assess and manage the risk if contact needs to be made with the applicant/ person at risk or the subject.

- **Are you concerned about the subject knowing you are making this application?** - This information is used to assess and manage the risk if contact needs to be made with the applicant/ person at risk or the subject.

- **If you are applying about someone else's partner does that person know you are making this application?**
  - This information is used to assess and manage the risk if contact needs to be made with the applicant/ person at risk or the subject.

- **Do you think there is an immediate risk that Police should act quickly on?** - This information will be used to identify if there are any urgent actions required by Police or other agency In order to safeguard the person at risk, children or subject.

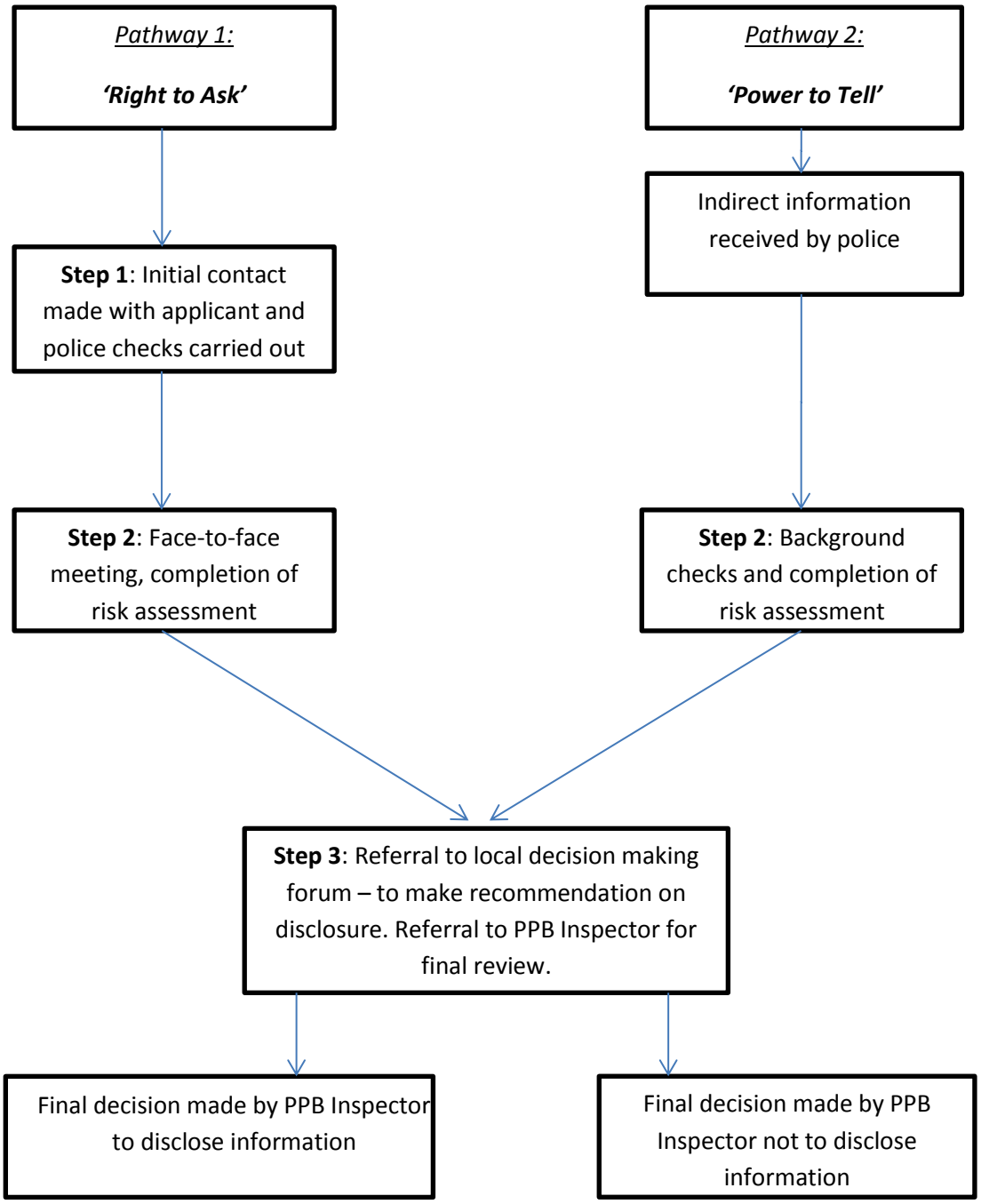
- **Is there anything else you feel Police should know? (Please inform us about any other risks, concerns or comments you might have.)** - Please complete this section if you have other information that has not been included in any other section of the application that you feel Police need to be aware in order to take appropriate actions to safeguard applicant, person at risk, children or subject. Police will only be able to act on information that they are aware of at the time.

DECLARATION

The lawful basis for the processing of this form comes from our duty to protect life and prevent crime (section 32 of the police (Northern Ireland) Act 2000, The right to life Article 2 Human Rights Act, The right to be free from torture, of inhumane and degrading treatment Article 3 Human Rights Act and Child Protection safeguarding ,The Childrens Order 1995, where the public interest in safeguarding the childs welfare overrides the need to keep the information confidential and the Data Protection Act.

ANNEX B

Flowchart: Overview of Domestic Violence and Abuse Disclosure Scheme



ANNEX C

Definitions

'A' – is the partner who is in, or was previously in, a relationship with a potentially violent and/or abusive individual ('B').

'B' – is the potentially violent and/or abusive individual who is/was in a relationship with a partner 'A'.

'C' – is a person who knows 'A' and who has concern for 'A's safety. This could include any third party such as a parent, neighbour or friend.

Applicant – means the person making the application under 'Right to Ask' ('A' or 'C').

Application – means those enquiries under 'Right to Ask' that go on to be processed as formal domestic violence and abuse disclosure applications, excluding applications that are not 'true' disclosure scheme applications i.e. vetting and barring, intelligence giving opportunities.

Disclosure – means the act of disclosing specific information to 'A' or 'C' about 'B's convictions; and/or any other relevant intelligence or information deemed necessary and proportionate to protect 'A' from harm.

Domestic violence and abuse definition – threatening, controlling, coercive behaviour, violence or abuse (psychological, virtual, physical, verbal, sexual, financial or emotional) inflicted on anyone (irrespective of age, ethnicity, religion, gender, gender identity, sexual orientation or any form of disability) by a current or former intimate partner or family member.

Indirect information – means that, under 'Power to Tell', the police come into possession of information that may impact the safety of 'A' and which has not been conveyed to the police via the 'Right to Ask' process.

Information-sharing – sharing of information between all the agencies (both statutory and non-statutory) involved in the Domestic Violence and Abuse Disclosure Scheme.

Relationship – is where the persons are 'personally connected' i.e. where both individuals are, or have been a couple, or otherwise in an intimate personal relationship with each other. This relationship does not necessarily have to involve a sexual element. .

Decision Making Forum (DMF) – means a multi-agency forum consisting of safeguarding agencies, PSNI, PBNI and third sector that is constituted to advise

whether disclosure would be appropriate in a particular case. DMF operates under the auspices of the existing MARAC process and procedures.

Harm – This incorporates the definition of harm as applied in the MARAC Operating Protocol (4 August 2014) - and includes the risk of harm (physical or psychological) which is life threatening and/or traumatic and from which recovery is usually difficult or incomplete.

ANNEX D

Principles underpinning DVADS

Information sharing and disclosure - overview

The successful implementation of DVADS is dependent, firstly, on appropriate information sharing between agencies and, secondly, on appropriate disclosure to a third party for the purpose of protecting the public.

Information sharing is the sharing of information between or among agencies involved in DVADS (both statutory and non-statutory) about an individual for the purpose of protecting a potential victim.

At all times, the power to both share and/or disclose information must be considered on a case-by-case basis, and each decision must be justifiable as being lawful i.e. necessary and proportionate.

As part of the disclosure process, information will be sought from partner agencies by PSNI and where there is information to be considered for disclosure, referral of the case will be made by PSNI to a multi-agency forum – known as a Decision Making Forum (DMF). DMF will operate under the auspices of the current Multi Agency Risk Assessment Conference (MARAC). MARAC is currently police-led, and this will be the case for DMF. It will be for PSNI to make the ultimate decision on whether or not to disclose the information under consideration. Agencies must ensure that, following a disclosure referral made to DMF, the information received is processed in accordance with the Human Rights Act 1998 and the Data Protection Act 1998, including the forthcoming General Data Protection Regulation.

DMF is not a 'data controller' (for the purposes of the Data Protection Act 1998). Rather, it is an arrangement for decisions to be taken on the management of risks it assesses are posed by the potential victim or the perpetrator. It, therefore, cannot be the owning agency for any information on the latter.

Information that is shared under DVADS remains the responsibility of the agency that holds it. For example, PBNI may hold certain information regarding their statutory supervision of a domestic abuse perpetrator, and PSNI may hold certain information regarding the separate management of a perpetrator.

This means that should a person request information held by an agency on them, then it will be for the relevant agency to deal with any Subject Access Request (SAR) made under the Data Protection Act 1998 and any other challenges that may arise. The proper approach to deal with a SAR does not form part of this guidance.

This section of the guidance should be read in conjunction with the Information Commissioner's Office (ICO) Data Sharing Code of Practice and ICO code on the DPA exemption in section 29 of the Data Protection Act regarding crime prevention. Both documents are available from the ICO website at www.ico.gov.uk. The code of practice deals with a number of important issues including: data sharing and the law; fairness and transparency; security; governance and individuals' rights. Officers engaged in the process should familiarise themselves with the contents of the document.

The power to share information

The purpose of sharing information about individuals is to enable the relevant agencies (both statutory and non-statutory) to work more effectively together in assessing risks and consider how to manage them. This points towards sharing all the available information that is relevant, so that nothing is overlooked and public protection is not compromised. However, there are certain principles that must be taken into account when considering whether to share information.

Information sharing must adhere to common law and legislation. Whilst ordinarily, non-statutory agencies are bound by common law duty of confidence, (which requires that information provided should not be used or disclosed further in an identifiable form, except as ordinarily understood by the provider, or with his or her subsequent permission), the law has established a defence to breach of confidence where disclosure is in the public interest. The prevention, detection, investigation and punishment of serious crime and the prevention of abuse or serious harm may well amount to a sufficiently strong public interest to override the duty of confidence.

Information sharing under DVADS must comply with the eight data protection principles set out in the DPA and reproduced in the ICO Code of Practice. Among other things, this means that the information shared must be accurate and up-to-date; it must be stored securely; and it must not be retained any longer than necessary. The DPA principles are set out at Annex E.

In normal circumstances, data shall be handled only with the data subject's consent, transparently, and only in ways which the data subject would reasonably expect. However, section 29 (1) of DPA provides an important exemption to the requirement to comply with the data principle 1, if the sharing of personal data is necessary for the prevention and detection of crime (guidance on section 29 is available on the ICO website).

Under DVADS, it will be appropriate for information to be shared under this exemption and without the consent of the data subject ('B'), if it can be shown that such sharing is necessary for the prevention of a crime against 'A'. However, in the case of personal data, a condition from Schedule 2 must be met and a condition from Schedule 2 and from Schedule 3 must be met in the case of sensitive personal

data. It is also important to note that such information shared must comply with the remaining data protection principles. Use of the exemption should be considered on a case-by-case basis.

Data sharing must also comply with the Human Rights Act 1998 (HRA): Articles 6 and 8 of ECHR, given domestic effect by HRA. Article 6 provides the right to a fair trial and would involve engagement with the subject's ('B's) rights under the scheme. Article 8 provides a right to respect for private and family life, home and correspondence. Any interference with this right by a public authority (such as a criminal justice agency), must be "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

The sharing of personal information about a potential perpetrator may be an interference with a person's right to a private and family life. To comply with Article 8 of the ECHR, any such interference must be shown to be necessary and proportionate in the pursuit of a legitimate aim, such as public safety, or the prevention of disorder or crime.

In human rights law, the concept of proportionality means doing no more than is necessary in pursuit of a legitimate aim. The third data protection principle provides that personal data must be relevant, and not excessive in relation to the purpose for which it is being shared.

Agencies must also respect the statutory rights of individuals including the right to privacy. In order to strike the right balance, agencies require a clear understanding of the law in this area. The most relevant factors are common law (where appropriate), section 32 of the Police (Northern Ireland) Act 2000, the Data Protection Act 1998 (including the forthcoming General Data Protection Regulation) and the Human Rights Act 1998.

<u>The power to disclose information</u>

The ability of DMF to recommend a disclosure of information must be decided on a case-by-case basis. Although the decision will, ultimately, rest with PSNI, it will be helpful for DMF to bear in mind that PSNI will require to be satisfied that any such disclosure is lawful, necessary and proportionate to justify the disclosure being made.

There is a general presumption that certain types of information held by PSNI about an individual will be treated sensitively and, in most cases, will be treated as confidential. That will include information about previous convictions, and possibly about spent convictions (in terms of the Rehabilitation of Offenders (NI) Order 1978).

It might also include information arising from dealings with the police which might not have led to a conviction, but where the individual might have been detained or arrested, and never charged or reported.

Additionally, it may include information where the individual has come to the adverse attention of the police because someone has made a complaint about them, or it may be intelligence which is held about an individual. All these types of information will be included, where relevant, for consideration in terms of DVADS.

Accordingly, when considering whether to recommend a disclosure of information, DMF should follow this 3 stage test:

- That DMF has the ability to recommend a disclosure of information by PSNI in terms of the 2000 Act. Such a disclosure would be lawful if accorded with one of the general policing duties in terms of the 2000 Act;

- PSNI must be able to show that it is reasonable to conclude that such disclosure is necessary to protect the public (or particular sections of the public) from crime; and

- In the context of the scheme, PSNI would have to conclude that disclosure to the applicant is necessary to protect 'A' from being a victim of a crime or abusive behaviour; and

- Any disclosure is an interference with the rights of 'B' (under Article 8 ECHR) and it must be proportionate;

- Where data is held by PSNI, there is a reasonable expectation that the information held will be afforded the rights of privacy, as protected by Article 8 ECHR;

- The principle of proportionality provides that whilst Articles 6 and 8 are necessary in a democratic society, the protection of vulnerable members within the community will demand that where there is a pressing social need to disclose information to ensure a vulnerable person's personal safety, this will occur only when there is an overriding public interest to do so. Using a rigorous process, an examination of the circumstances will be considered relative to the threat presented. Only after all factors have been considered and the threat carefully assessed, will a decision be made to disclose information;

- This involves weighing in the balance the likely consequences for 'B' if certain details about him/her are disclosed against the nature and extent of the risks that 'B' poses to 'A';

- This stage of the test also involves considering the extent of the information which needs to be disclosed e.g. it may not be necessary to tell the applicant the precise details of the offence for the applicant to take steps to protect 'A'. There must be a balance of the rights of 'B' against the need to prevent crime and all decisions in this regard must be fully documented.

Other principles

The following other principles also underpin DVADS at every stage of the process:

- DVADS endeavours to advance a model for the assessment sharing and possible disclosure of information about those with a history of domestic violence and abuse to assist those who might yet become victims of same. It also endeavours to raise public confidence and increase the protection of potential victims of domestic violence and abuse by sharing relevant sources of information showing, or tending to show, that an individual has a history of domestic violence and abuse. Such information will be judged based on a risk assessment and, where appropriate, the National Intelligence Model;

- No disclosures should be made without following all appropriate stages of this guidance document (unless there is an identified immediate/imminent risk of harm to the potential victim, as per Articles 2 and 3 ECHR);

- At all times, consideration must be given to the safety of the potential victim with appropriate actions (e.g. safety planning, information on safeguarding) implemented, followed through and recorded;

- Under the 'Right to Ask' route, if at any stage PSNI believe that the applicant is alleging a crime (e.g. a specific incidence of domestic violence and abuse), then PSNI must also pursue the crime report under normal criminal investigation procedures;

- Subject to the processes outlined in this document being met in full, including the data sharing and disclosure process mentioned earlier. A disclosure will be made to the potential victim, unless there is a compelling reason(s) not to, for example the potential victim is considered too vulnerable to understand the consequences of the disclosure. In such circumstances, disclosure will be made to the person best able to safeguard the potential victim, as determined by the level of risk identified (e.g. relative, social worker).

ANNEX E

Data Protection Act 1998 Principles

This annex contains information and further guidance on applying the 8 principles of the Data Protection Act 1998. This information and further information on the Data Protection Act can be obtained from the Information Commissioner's Office and is available at www.ico.gov.uk

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Personal data shall be accurate and, where necessary, kept up to date.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Further guidance on applying the Data Protection Act principles

1. The Data Protection Act says that:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a) At least one of the conditions in Schedule 2 is met, and
b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first data protection principle. In practice, it means that you must:

- Have legitimate grounds for collecting and using the personal data;
- Not use the data in ways that have unjustified adverse effects on the individuals concerned;
- Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- Handle people's personal data only in ways they would reasonably expect; and
- Make sure you do not do anything unlawful with the data.

Section 29 of the DPA provides an important exemption to this requirement if the sharing of personal data is necessary for the 'prevention and detection of crime'. However, in the case of personal data, a condition from Schedule 2 must be met and a condition from Schedule 2 **and** a condition from Schedule 3 must be met in the case of sensitive personal data. Such information shared must comply with the remaining data protection principles. Use of the exemption should be considered on a case-by-case basis.

2. <u>The Data Protection Act says that</u>:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

This requirement (the second data protection principle) aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

There are clear links with other data protection principles – in particular the first principle, which requires personal data to be processed fairly and lawfully. If you obtain personal data for an unlawful purpose, for example, you will be in breach of both the first data protection principle and this one. However, if you comply with your obligations under the other data protection principles, you are also likely to comply with this principle, or at least you will not do anything that harms individuals.

In practice, the second data protection principle means that you must:

- Be clear from the outset about why you are collecting personal data and what you intend to do with it;

- Comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- Comply with what the Act says about notifying the Information Commissioner; and
- Ensure that if you wish to use or disclose the personal data for any purpose that is additional to, or different from, the originally specified purpose, the new use or disclosure is fair.

3. The Data Protection Act says that:

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This is the third data protection principle. In practice, it means you should ensure that:

- You hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- You do not hold more information than you need for that purpose.

4. The Data Protection Act says that:

Personal data shall be accurate and, where necessary, kept up to date.

This is the fourth data protection principle. Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

- Take reasonable steps to ensure the accuracy of any personal data you obtain;
- Ensure that the source of any personal data is clear;
- Carefully consider any challenges to the accuracy of information; and
- Consider whether it is necessary to update the information.

5. The Data Protection Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is the fifth data protection principle. In practice, it means that you will need to:

- Review the length of time you keep personal data;

- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

6. The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. The Act says that:

Personal data shall be processed in accordance with the rights of data subjects under this Act.

This is the sixth data protection principle, and the rights of individuals that it refers to are:

- A right of access to a copy of the information comprised in their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to claim compensation for damages caused by a breach of the Act.

7. The Data Protection Act says that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to, personal data.

This is the seventh data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- Design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- Be clear about who in your organisation is responsible for ensuring information security;
- Make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- Be ready to respond to any breach of security swiftly and effectively.

8. The Data Protection Act says that:

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using subcontractors abroad.

The Act also sets out the situations where the eighth principle does not apply, and these situations are also considered in more detail in this section.