

Domestic Violence Disclosure Scheme

Contents

| | |
|---|----|
| 1. Introduction..... | 2 |
| 2. Aims..... | 4 |
| 3. Definitions..... | 8 |
| 4. Principles underpinning the Domestic Violence Disclosure Scheme..... | 9 |
| Information sharing and disclosure - overview | 9 |
| <i>The ability to share information</i> | 9 |
| <i>The ability to disclose information</i> | 11 |
| <i>Other principles</i> | 11 |
| 5. The Process | 14 |
| “Right to Ask” entry route..... | 14 |
| Step 1 – Initial Contact with Police..... | 14 |
| Step 2 – Face to Face Meeting | 18 |
| Step 3 - Full risk assessment..... | 19 |
| “Right to Know” entry route | 21 |
| Referral to local decision-making forum..... | 22 |
| <i>Categorising a “concern” or “no concern</i> | 22 |
| <i>Principles the local decision making forum must consider when making a decision on whether to disclose</i> | 23 |
| Decision made to disclose information..... | 24 |
| Decision made not to disclose information | 25 |
| Managing the perpetrator | 26 |
| Maintaining a record of the Disclosure Scheme | 26 |
| Annex A – Non-exhaustive list of offences where convictions and/or allegations may be disclosed under the Domestic Violence Disclosure Scheme | 27 |
| Annex B – Data Protection Act 1998 Principles..... | 29 |
| Annex C – Template of Minimum Standard of Information to be Obtained and Checks to be Completed at the Initial Contact Stage | 33 |
| Annex D – Template for Initial Checks/Risk Assessment | 35 |
| Annex E – Template for face-to-Face contact meeting | 37 |
| Annex F – Template checklist on disclosure decision making process by the local decision making forum | 39 |
| Annex G – Template containing minimum information to be disclosed (including form of words)..... | 41 |
| Annex H – Template form of words for non-disclosure | 44 |

1. Introduction

- 1) This guidance document has been developed to support the implementation of the Domestic Violence Disclosure Scheme. Approximately two people are killed by their current or former partner each week in England and Wales. The case of Clare Wood, who was murdered by her former partner in Greater Manchester in 2009, brought to national attention the issue of disclosing information about an individual's history of domestic violence to a new partner. Noting that her former partner had three previous convictions under the Protection from Harassment Act 1997, the Coroner's report into the murder published in July 2011 contained the following recommendation:

subject to appropriate risk assessment and safeguard, I recommend that consideration should be given to the disclosure of such convictions and their circumstances to potential victims in order that they can make informed choices about matters affecting their safety and that of their children.

- 2) The tragic case of Clare Wood follows a report commissioned by the Home Office and published in 2009 by Chief Constable Brian Moore of Wiltshire Police on behalf of the Association of Chief Police Officers (ACPO) - *Tackling Perpetrators of Violence against Women and Girls*. Chief Constable Moore set out a series of ten recommendations which included a "right to know" where he concluded that *"whilst routine disclosure should not be common practice, following risk assessment it may be proportionate and necessary to enable a potential victim to make choices about her safety and that of her children."*
- 3) On 25th October 2011, the Government launched a consultation inviting views from the public on whether the protection of victims of domestic violence could be enhanced by the establishment of a national Domestic Violence Disclosure Scheme that had recognised and consistent procedures for disclosing information to enable new partners of previously violent individuals to make informed choices about how and whether they take forward that relationship. The consultation closed on 13th January 2012 and, having carefully considered the 259 response received to the consultation, the Home Office announced that the Domestic Violence Disclosure Scheme would be tested in a one-year pilot from the summer of 2012 in four police force areas – Greater Manchester, Gwent, Wiltshire, and Nottinghamshire. The disclosure process will be tested within existing police legislative powers to share information and to ensure that appropriate risk assessments and safeguards are in place to accommodate the issues raised by this consultation.
- 4) The Home Office gratefully acknowledges the following sources during the development of this guidance document: *The Child Sex Offender (CSO) Disclosure Scheme Guidance Document*, the *MAPPa Guidance 2012 Version 4*, and members of the Domestic Violence Disclosure Scheme Steering Group set up by the Home Office.

What is new about the Domestic Violence Disclosure Scheme?

- 5) The Domestic Violence Disclosure Scheme provides the following benefits:
 - a. introduces recognised and consistent procedures for disclosing information that enables a new partner (known as "A" throughout this document) of a previously violent individual (known as "B" throughout this document) make informed choices about whether and how A takes forward that relationship with B;
 - 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", individual members of the public can now proactively seek information, with an expectation that the agencies responsible for safeguarding victims of domestic violence will check to see whether relevant information exists and if it does, that consideration will be given to its disclosure where necessary to protect the victim;
 - d. under "right to know", where a safeguarding agency comes into the possession of information about the previous violent behaviour of a person (B) that may cause harm to another person (A), 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, necessary and proportionate to protect the potential victim from further crime;
- e. encourages individuals to take responsibility for safety of the victim.

What is the same?

- 6) The Domestic Violence Disclosure Scheme has not introduced any new legislation. Therefore, any disclosure must be within the existing legal framework and, in particular, have due regard to established case law, the Human Rights Act 1998, the Data Protection Act 1998 and the Rehabilitation of Offenders Act 1974. Further guidance on this is given under the heading "Principles underpinning the Domestic Violence Disclosure Scheme".

2. Aims

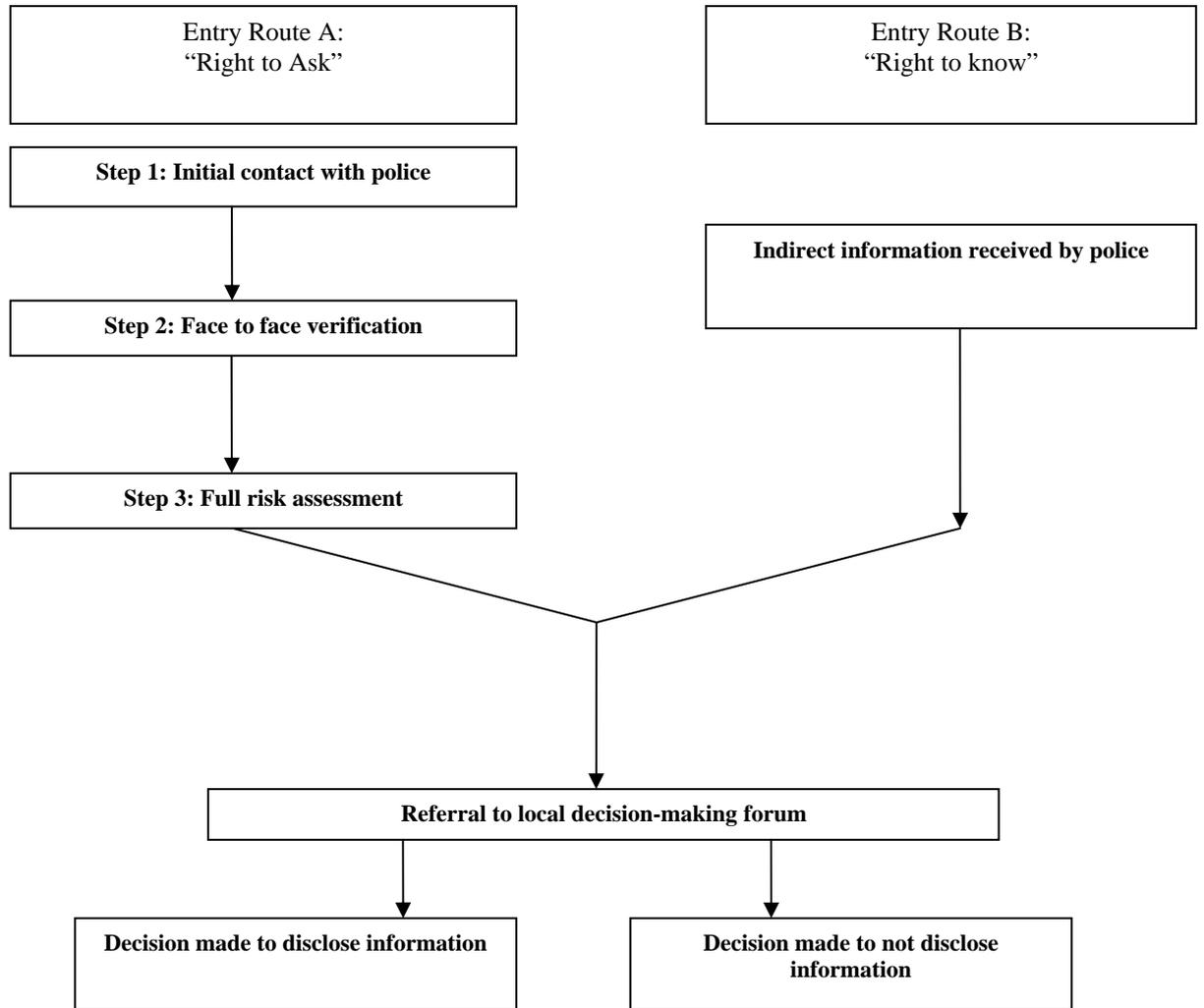
- 7) The principal aim of the Domestic Violence Disclosure Scheme is to introduce recognised and consistent procedures for disclosing information which will enable a partner (A) of a previously violent individual (B) make informed choices about whether and how A takes forward that relationship with B. **Critical to the success of the Domestic Violence Disclosure Scheme is the need for a risk assessment to be completed at every stage in the disclosure process**, as the risk assessment will inform the practical actions necessary to safeguard A and to inform the development of a potential disclosure under this Scheme.
- 8) The Domestic Violence Disclosure Scheme articulates two distinct entry routes that may lead to a disclosure being made. The first entry route – “right to ask” – is modelled closely on the existing Child Sex Offender Disclosure Scheme, and is triggered when a person makes a *direct application* to the police for information about B. The second entry route – “right to know” – is triggered when the police receive *indirect* information or intelligence about the safety of A and where, after appropriate checks are made, the police judge that a disclosure should be made to safeguard A. Certain stages of the Domestic Violence Disclosure Scheme are common to both entry routes and, accordingly, the Disclosure Scheme may be visualised in Figure 1.
- 9) The Disclosure Scheme is focussed on disclosure and risk management where B is identified as having convictions (including cautions, reprimands and final warnings) for violent offences; and/or information held about B’s behaviour which reasonably lead the police and other safeguarding agencies to believe that B poses a risk of harm to A.
- 10) This Guidance document provides:
 - a. checks to be completed;
 - b. a set of minimum standards of information to be obtained from the applicant;
 - c. suggested forms of wording for communicating outcomes at each stage of the Disclosure Scheme process;
 - d. recommended minimum levels of knowledge and experience required by practitioners to discharge functions within the Disclosure Scheme effectively.
- 11) It is important to all involved in delivering this scheme that potential or actual victims of domestic violence are protected from harm. By making a request for disclosure, a person will often also be registering their concerns about possible risks to the safety of A. For that reason, it is essential to this process that police forces work closely with the local Multi-Agency Risk Assessment Conference (MARAC) or, where not available, other suitable local safeguarding forum, to ensure that any possible risks of harm to A are fully assessed and managed.
- 12) This scheme does not replace existing arrangements for Criminal Records Bureau (CRB) checks, Subject Access or Freedom of Information (FOI) requests, or the proposed new Disclosure and Barring Service. If it is identified at the initial contact that the request is one of these other types of enquiry then it should be directed down the existing route for this type of request.

What happens in areas not yet implementing the Domestic Violence Disclosure Scheme?

- 13) Although the Domestic Violence Disclosure Scheme is being piloted in four police areas initially, anyone who has concerns about the safety of person at risk of domestic violence should go to any police force at any time about their concerns. Every police force has a public protection team to deal with these issues. In all areas (whether covered by the scheme or not), the police have a common law power to disclose information where it is necessary to prevent a crime. Furthermore, the police’s ability to make the disclosure is not dependent on a request from the public. *(Special note: a member of public residing in a non-pilot police force who has concerns about a potential victim (A) who resides in a pilot area will be referred*

to the relevant pilot police force area where the application will be progressed. A non-pilot police force will process all other requests according to its local procedures).

Figure 1: Overview of Domestic Violence Disclosure Scheme entry routes



3. Definitions

14) The following definitions are used for the purposes of this guidance document:

A – is the partner who is in an intimate relationship with a potentially violent individual (B).

applicant – means the person making the application under “right to ask”.

application – means those enquiries under “right to ask” that go on to be processed as formal domestic violence disclosure applications, excluding applications that are not ‘true’ disclosure scheme applications i.e. vetting and barring, intelligence giving opportunities.

B – is the potentially violent individual who is in an intimate relationship with a partner (A).

C - is a third party who has some form of contact with A. This could include any third party such as a parent, neighbour or friend. This is to ensure any safeguarding concerns are thoroughly investigated. However, a third party making an application will not necessarily receive a disclosure as a more appropriate person to receive disclosure may be A or a person deemed by the risk assessment as the person best placed to safeguard A (e.g. parent, third-sector worker).

decision-making forum - means the local forum consisting of safeguarding agencies, police, probation and third sector that is constituted to consider making a disclosure. Ideally, this should be the Multi-agency Risk Assessment Conference (MARAC) or, where this is not possible, another appropriate forum that local needs determine and which can deliver the intended outcomes of the Domestic Violence Disclosure Scheme

disclosure – means the act of disclosing information about the B’s convictions for violent offence and any other relevant information deemed necessary and proportionate to protect A from harm.

indirect information – means that, under “right to know”, 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.

intimate relationship – means a relationship between two people which may be reasonably characterised as being physically and emotionally intimate.

serial perpetrator – for the purposes of this Disclosure Scheme, the definition articulated by the Crown Prosecution Service is used

where a suspect has committed an act of domestic violence against two or more different victims or complainants they should be considered a 'serial perpetrator'.

violent offence – means an offence which leads, or is intended or likely to lead, to a person’s death or to physical injury to a person. Annex A of this guidance document gives a non-exhaustive list of offences that may be disclosed under the Domestic Violence Disclosure Scheme.

4. Principles underpinning the Domestic Violence Disclosure Scheme

Information sharing and disclosure - overview

- 15) The successful implementation of the Domestic Violence Disclosure Scheme is dependent on appropriate **information sharing** between agencies and **disclosure** to a third party for the purpose of protecting the public. The police have a common law power to disclose information where it is necessary to prevent and detect a crime, and it is on this common law power that the authority of the police to disclose information under the Domestic Violence Disclosure Scheme rests. However, this common law power must be exercised in accordance with statutory obligations. This section of the guidance document gives an overview of the principles that all agencies (both statutory and non-statutory) who are involved in the Domestic Violence Disclosure Scheme must consider on every occasion when a potential disclosure arises.
- 16) At all times, the ability to both share and disclose information must be considered on a case-by-case basis to determine whether the sharing and disclosure of information is lawful, necessary and proportionate. For the sake of clarity, **information sharing** is the sharing of information between all the agencies (both statutory and non-statutory) involved in the Domestic Violence Disclosure Scheme. **Disclosure** is the sharing of specific information about a person (known as B in this guidance document) with a third party (known as either A or C in this guidance document) for the purpose of protecting the public (envisaged to be A in this guidance document). The third party could be a member of the public such as a victim, a person forming an intimate relationship with an offender, or a person acting in a professional capacity but not party to the Domestic Violence Disclosure Scheme arrangements. A **potential disclosure** is a situation where the local decision-making forum is considering whether to disclose information following an application made under the “right to ask” entry route or indirect information received under the “right to know” entry route.
- 17) Information that is shared under the Domestic Violence Disclosure Scheme remains the responsibility of the agency that holds it. For example, the Probation Service will hold information regarding their statutory supervision of a perpetrator, and the police hold information regarding their separate management of a perpetrator. Should a person request information held by an agency on them, then it will be for the relevant agency to deal with Subject Access Requests under the Data Protection Act 1998 and other challenges that may arise. The local decision-making forum as such is not an organisation, but an arrangement for managing the risks posed to A by B. It therefore cannot be the owning agency for any information on B. Agencies must ensure that, following a disclosure decision made by the decision-making forum, the information received as part of that decision-making process is processed in accordance with the Data Protection Act 1998.
- 18) This section of the guidance should be read alongside the Data Sharing Code of Practice issued by the Information Commissioner in May 2011. It is available from the website of the Information Commissioner’s Office (“ICO”) which is at <http://www.ico.gov.uk>. The code of practice deals with a number of important issues such as Data Sharing and the Law; Fairness and Transparency; Security; Governance; and Individuals’ Rights. It is a statutory code. Although it is not binding, it can be used in evidence in legal proceedings.

The ability to share information

- 19) The purpose of sharing information about individuals (“data subjects”) is to enable the relevant agencies (both statutory and non-statutory) to work more effectively together in assessing risks and considering 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. On the other hand, agencies (both statutory and non-statutory) must also respect the statutory rights of data subjects. In order to strike the right balance, agencies need a clear understanding of the law in this area. The most relevant factors are common

law, the Data Protection Act 1998 (“DPA 1998”) and the Human Rights Act 1998 (“HRA 1998”). The principles derived from this legislation may be summarised as follows.

- 20) Firstly, information-sharing must be lawful. This means, first, that the sharing of information must be in accordance with the law. Whilst ordinarily non-statutory agencies are bound by a common law duty of confidence (which requires that information provided should be used or disclosed further in an identifiable form except as originally understood by the provider, or with his or her subsequent permission), case law has established a defence to breach of confidence where the breach is in the public interest. The prevention, detection, investigation and punishment of serious crime and the prevention of abuse or serious harm will usually be sufficiently strong public interests to override the duty of confidence.
- 21) Secondly, the information-sharing must comply with the eight Data Protection Principles set out in the DPA 1998 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. Data principle 1 of the DPA 1998 also specifies that the 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.

In normal circumstances, this means data shall be handled with the data subject’s consent, transparently, and only in ways which the data subject would reasonably expect. However, section 29(1) of the DPA 1998 provides an important exemption to the requirement to comply with data principle 1 if the sharing of personal data is necessary for the *prevention and detection of crime*. Under the Domestic Violence Disclosure Scheme, it will be appropriate for information to be shared under this exemption and without the consent of the data subject (in this instance B) if it can be shown that such sharing is necessary for the prevention of a crime against A. However, it is also important to note that such information shared must comply with the remaining data protection principles – in other words, that the information shared is accurate and up-to-date, is stored securely, is not retained for any longer than necessary etc.

- 22) Thirdly, the information-sharing must be necessary. Article 8 of the European Convention on Human Rights, given domestic effect by the HRA, 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.”
- 23) 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 European Convention on Human Rights, any such interference must be shown to be necessary and proportionate in the interests of public safety or for the prevention of disorder or crime.
- 24) Fourthly, information-sharing must be proportionate. In human rights law, the concept of proportionality means doing no more than is necessary to achieve a lawful and reasonable result. 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.
- 25) For the purposes of the Domestic Violence Disclosure Scheme, this essentially means ensuring that information about the data subject is relevant to assessing and managing risk and that no more information is shared than is needed to manage that risk. For example, if what is actually needed is the names and addresses of individuals, sharing their race and religion as well would be likely to be disproportionate.

- 26) Although the exchange of information between non-statutory agencies that form the local decision-making forum has to be considered on a case-by-case basis, formal protocols or agreements should be in place in advance if possible. These agreements should pay particular attention to ensuring the safety and security of the personal information shared. Sections 8 and 14 of the ICO Code of Practice are concerned with the issues that an information-sharing agreement should cover. These include what information is to be shared, with whom, and why; the quality and security of the information; the circumstances governing the length of time for which the information is retained; and what happens if the agreement is breached.

The ability to disclose information

- 27) The ability of the local decision making forum to disclose information under the Domestic Violence Disclosure Scheme must be done on a case-by-case basis, and the local decision making forum must consider that it is lawful, necessary and proportionate to justify the disclosure being made. This approach is dependent upon agencies (both statutory and non-statutory) having due regard to all of the following:
- a. whether there is the power to disclose the information (whether under statute of the common law)
 - b. common law duty of confidence
 - c. Article 8 of the European Convention of Human Rights
 - d. Data Protection Act 1998
 - e. Rehabilitation of Offenders Act 1974
- 28) There is a general presumption that intelligence on a person or details about a person's previous convictions are confidential. Accordingly, when considering whether to disclose information, the local decision-making forum must apply the following 3 stage test is satisfied before a decision to disclose is made:
- a. that the local decision making forum has the power to disclose the information. As the Domestic Violence Disclosure Scheme is reliant on common law powers, then the police must be able to show that it is reasonable to conclude that such disclosure is necessary to protect the public from crime. In the context of this scheme, the police would have to conclude that disclosure to the applicant is necessary to protect A from being the victim of a crime related to domestic violence (see Annex A for list of relevant offences);
 - b. that there is a pressing need for such disclosure; and
 - c. interfering with the rights of the offender (under Article 8 of the European Convention of Human Rights) to have information about his/her previous convictions kept confidential, is necessary and proportionate for the prevention of crime. This involves considering the consequences for B if his/her details 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.
- 29) More detailed guidance on these issues is provided under the section entitled "Disclosure decision made and discharged". Annex B provides guidance on how to apply the Data Protection Act principles.

Other principles

- 30) The following other principles also underpin the Domestic Violence Disclosure Scheme at every stage of the process:

- a) No disclosures should be made to members of the public in respect of an individual's previous convictions or intelligence history without following all appropriate stages of this guidance document (unless there is an immediate/imminent risk of harm to A).
- b) At all times, consideration must be given to the safety of A with appropriate actions (e.g. safety planning, information on safeguarding) implemented and followed through.
- c) Under the "right to ask" entry route, if at any stage the police believe that the applicant is alleging a crime (e.g. a specific incidence of a violent act by B on A), then the police must pursue the crime report under normal criminal investigation procedures.
- d) Subject to the processes outlined in this document being met in full (and, in particular, the data sharing and disclosure considerations as articulated in paragraphs 15-29 above), there is an assumption that a disclosure will be made to A unless there is a compelling reason not to – for example, the risk assessment flags that a disclosure to A would put A in danger; A does not have the mental capabilities to understand the consequences of the disclosure. In such circumstances, disclosure will be made to the person best able to safeguard A as determined by the risk assessment (e.g. relative, social worker).
- e) To raise public confidence and increase the protection of victims of domestic violence, both convictions for violent offences and/or relevant intelligence where it is judged that B poses a risk of harm to A may be disclosed. Such a judgement will be based on a risk assessment and, where intelligence is disclosed, the National Intelligence Model. Information disclosed may include:
 - i. un-spent convictions held by B on any offence related to domestic violence (see annex A for guidance on offences that may be disclosed);
 - ii. information where, even if B does not possess any convictions, it indicates that B poses a risk of harm to A.
- f) Information on spent convictions as defined under the Rehabilitation of Offenders Act 1974 may not be disclosed – this includes spent convictions that are from overseas. **It will be for the decision making forum to check on a case-by-case basis whether a specific offence on which B has been convicted is spent or not before a disclosure is made.** However, it is permissible for the police and other agencies to consider the impact of a spent conviction when determining a risk assessment on A, regardless of the fact that the spent conviction may not subsequently be disclosed.
- g) Table 1 specifies the maximum timescales to be observed under the "Right to Ask" and "Right to Know" entry routes.

Table 1 – Maximum Timescales

| "Right to Ask" | | "Right to Know" | |
|---|--|-------------------------------|--|
| Initial Contact made | | Indirect information received | |
| Step 1 – Initial Contact checks | Completed within 24 hours from Initial Contact made | | |
| Step 2 – face – face meeting | Completed within 10 working days from Initial Contact checks | | |
| Step 3 – full-risk assessment | Completed within 5 working days from face-to-face meeting | Minimum checks made | Completed within 5 working days from indirect information received |
| Referral to local decision making forum occurs no later than 20 working days from "Step 3 – full risk assessment" (under "right to ask") or "Minimum checks made" (under "right to know") | | | |

5. The Process

“Right to Ask” entry route

Step 1 – Initial Contact with Police

Circumstances leading to an initial contact being made with the police

- 31) For the purposes of the “right to ask” entry route, the trigger that may lead to a disclosure under this scheme is where a person makes a direct application to the police for information about the previous violent behaviour of B.
- 32) For the purposes of this guidance document, a distinction is made where the applicant is either the partner (known as A) who is in an intimate relationship with B, or is a third party (known as C) who has some form of contact with A. This could include any third party such as a parent, neighbour or friend. This is to ensure any safeguarding concerns are thoroughly investigated. However, a third party making an application will not necessarily receive a disclosure as a more appropriate person to receive disclosure may be A or a person deemed by the risk assessment as the person best placed to safeguard A (e.g. parent, third-sector worker).
- 33) The direct application will be deemed to have been made when either A or C makes contact with the police by one of the following means:
 - a. A or C attends a police station in person;
 - b. A or C encounters a police officer/member of police staff in the street;
 - c. A or C makes direct contact as part of a police investigation to an incident;
 - d. A or C makes direct telephone call to the police
 - e. A or C emails the police
 - f. A or C makes an on-line report to the police (if available).

AND A or C asks for specific information about B’s previous violent offending.

- 34) **If at any stage during the initial contact the police believe that A or C is alleging a crime (e.g. a specific incidence of a violent act) rather than asking for information about the previous violent offending of B, then the police must pursue the crime report under normal criminal investigation procedures.** However, it is possible for the procedures leading to a disclosure under this Domestic Violence Disclosure Scheme to run concurrently with a criminal investigation triggered by the allegation of the crime.
- 35) If A or C makes an enquiry to a partner agency rather than the police, 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 Domestic Violence Disclosure Scheme, then A or C should be referred to the police. Initial contact can be made with the police by any of the above methods outlined in paragraph 33 above. A partner agency may facilitate contact with the police if it is appropriate.
- 36) If A or C visits a police station in person, then they must be allowed the opportunity to make their referral in private, as they may feel uncomfortable doing so in hearing of other members of the public.

Information to be obtained and communicated during the Initial Contact

- 37) It is envisaged that the initial contact by A or C will be received and managed by police control room staff. Where front-line police officers and Police Community Support Officers receive a verbal application during the course of their normal policing duties, they should record basic details of A or C and then make a referral to the control room staff to complete the initial contact.

38) After receiving the initial contact, the control room staff should take the following details from A or C:

- a. Details of A or C
 - i. Name (including any other names used: e.g. maiden)
 - ii. Date of Birth
 - iii. Place of Birth
 - iv. Address
 - v. Ethnic Origin
 - vi. Gender
 - vii. Preferred Language
- b. Preferred method of contact
 - i. Time
 - ii. Day
 - iii. Method (e.g. by telephone, face-to-face)
 - iv. Safety issues (e.g. applicant nominating a time and place when it is safe for the police to contact A or C)
- c. Details of B
 - i. Name (including any other names used)
 - ii. Date of Birth
 - iii. Place of Birth
 - iv. Address
 - v. Ethnic Origin
 - vi. Gender
 - vii. Place of work / employment
 - viii. Nature of relationship to A
- d. Details of children
 - i. Name (including any other names used)
 - ii. Date of Birth
- e. Details of registered interest
 - i. Information only – no domestic violence concerns
 - ii. B's behaviour as observed by the applicant
 - iii. B's behaviour as observed by a third party and relayed to the police by the applicant
- f. Elements of risk
 - i. Does B know that the applicant is making the enquiry?
 - ii. Consequences of B knowing that the applicant has made the enquiry.
- g. Consent to share personal data with other agencies *Note: it should be explained that the information gathered during the initial contact may be shared without consent if sharing the information is necessary to prevent a crime being committed against A.*

A template form containing this information is provided at Annex C. **Note: it is vital that, during this initial contact, a safe means of communication is agreed with A or C where the place, means and timing is determined by A or C. This is critical to safeguarding A.**

39) During the initial contact stage, the police member of staff should also inform A or C of the following:

- a. the Domestic Violence Disclosure Scheme does not replace existing procedures that are currently in place for Criminal Records Bureau (CRB) checks, subject access or Freedom of Information (FOI) requests and the proposed new Disclosure and Barring Service;

- b. a disclosure will only be made to the person who is in the best position to safeguard A from harm. This will normally be A, unless there is a compelling reason not to disclose to A;
- c. initial checks will be completed as soon as possible and, in any case, within 24 hours to:
 - i. assess whether the disclosure application should be progressed;
 - ii. assess whether there is an immediate or imminent risk of harm to A from B;
- d. should a decision be made to progress the disclosure application further:
 - i. the disclosure application will be referred to the police's Public Protection Unit to follow up;
 - ii. A or C will be required to undertake a face-to-face meeting within the next 10 working days;
- e. at the face-to-face meeting, A or C will be required to provide proof of their identity and, if the applicant is C, proof of their relationship to A;
- f. the police will aim to complete the enquiry within 35 days but there may be extenuating circumstances that increase this timescale. A or C will be informed if this is the case.
- g. if any immediate risks to A are identified at any stage, then immediate safeguarding action will be taken and this will include a robust safety plan delivered by the police and partners. Should a decision be made to disclose information to A, then this will also be accompanied with a robust safety plan tailored to the needs of A.

Minimum checks following Initial Contact

- 40) Following the initial contact, minimum checks should be undertaken by a police member of staff in accordance with local police procedures¹ to build an initial picture on A, B and C. The minimum standard of checks at this stage are:
- a. Police National Computer (PNC);
 - b. Police National Computer (PND)
 - c. ViSOR (if the subject has a ViSOR marker on the Police National Computer);
 - d. local intelligence systems.

These checks must not be made in the presence of A or C, to avoid any inappropriate or accidental disclosure to the person at this stage. No disclosure to A or C should be given by the staff member taking the initial contact details at this stage.

Decision on whether to progress Disclosure Application

- 41) The information gathered via the Initial Contact and Minimum Checks form both the initial risk assessment on A and the basis of a decision on whether to progress the Disclosure Application. **A template risk assessment form is at Annex D to assist this decision-making process.**
- 42) In accordance with local police procedures, it will be for the police member of staff to:
- a. make the decision on whether to progress the disclosure application following this risk assessment;
 - b. determine how A or C will be contacted to progress the disclosure application.

¹ The checks may be undertaken by police control room staff, or staff from the Public Protection Unit, or other appropriately trained staff, as local police procedures determine.

From the above steps outlined above, if it is identified there is an immediate/imminent risk of harm to A, then ACTION MUST BE TAKEN IMMEDIATELY to safeguard those at risk.

Step 2 – Face to Face Meeting

- 43) If following the risk assessment conducted under step 1, the police decide that the disclosure application should continue, the person who made the application (either A or C) must be seen in a face to face meeting. This is to ensure that the request is:
- genuine and not malicious; and
 - to establish further details about the application in order to further assess risk and to inform a decision around disclosure; and
 - to provide safety information and advice to safeguard A.

The face to face meeting should take place as soon as practicable and, in any event, no later than 10 working days after the initial contact.

- 44) It is highly recommended that police officers or members of police staff from the public protection unit should complete this stage of the process, as they will have experience and knowledge of managing domestic violence offenders and investigation into domestic violence incidents. This requisite knowledge and experience in this high-risk area of public protection will inform the relevant questioning and assist in assessing risk.
- 45) **If at any stage during the initial contact the police believe that A or C is alleging a crime (e.g. a specific incidence of a violent act) rather than asking for information about the previous violent offending of B, then the police must investigate the crime report and follow local procedures.** However, it is possible for the procedures leading to a disclosure under this Domestic Violence Disclosure Scheme to run concurrently with the criminal investigation.

Preliminaries

- 46) Before progressing enquiries on the application, the police member of staff must:
- warn A or C that if they wilfully or maliciously provide false information to the police in order to try and get 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(2) of the Criminal Law Act 1967 (*where a person causes any wasteful employment of the police by knowingly making to any person a false report tending to show that an offence has been committed, 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 if they disclose evidence of an offence whilst registering a concern, it may not be possible to maintain their confidentiality;
 - warn A or C that information disclosed by the police must only be used for the purpose for which it has been shared i.e. in order 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 process. It should be explained that in the event of a concern arises on B and a resultant disclosure is made to either A or C then, subject to the outcome of a risk assessment, B may have to be informed that a disclosure has been made to the applicant.
 - ask the A or C for proof of identity. Acceptable forms of ID may include:
 - passport;
 - driving licence;
 - other trusted form of photo identification;

- iv. birth certificate;
- v. household utility bill (electricity, gas, council tax, water);
- vi. bank statement.

- 47) Recommended best practice is that photo identification with confirmation of date of birth and address is required. However, it is accepted that some of the vulnerable individuals who may 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. social worker, health visitor).
- 48) **A disclosure must not 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.

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

- 49) The police member of staff should take the following details from A or C:

- a. Details of A or C
 - i. Name (including any other names used: e.g. maiden)
 - ii. Date of Birth
 - iii. Place of Birth
 - iv. Address
 - v. Ethnic Origin
- b. Further details
 - i. Reason for contact
 - ii. History of relationship between A and B

A template form containing this information, plus the warnings articulated in paragraph 46, is provided at Annex E.

- 50) A or C should be told that the person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and 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 is breach under 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 the police). This should be explained to the person and their signature obtained on this undertaking. If the person is not willing to sign the undertaking the police will need to consider if disclosure should still take place. The outcome should be recorded and considered in the subsequent risk assessment and decision making process.
- 51) After the face to face meeting, the applicant should be given an information pack on the Disclosure Scheme, which should give information on what they can do in the interim to better safeguard A pending the outcome of the application. The contents of the information pack is at the discretion of the police but should as a minimum contain:
- a. Leaflet to explain Domestic Violence Disclosure Scheme
 - b. local leaflets that provide sign-posts to local support services

Step 3 - Full risk assessment

- 52) Following the face-to-face meeting, the police should then consider conducting a full risk assessment according to the following scenarios.

Scenario 1: the original applicant is A

53) Under Scenario 1, the *Domestic Abuse, Stalking and Harassment and Honour Based Violence* (DASH) form should be fully completed and reference made to existing guidance issued by the Association of Chief Police Officers (ACPO) on domestic violence. Completion of the DASH form is vital to establish an appropriate safety plan for A.

54) The population of the DASH form should include revisiting the information obtained:

- a. in the initial contact
- b. at the face to face stage
- c. on the Police National Computer,
- d. on the Police National Database,
- e. VISOR,
- f. local intelligence systems.

The research and checks should aim to fill any gaps in information and this stage should ensure all available information known to police on the individuals concerned with the enquiry has been established.

55) Checks will also be completed with other agencies where appropriate. This will include:

- a) social services (where the applicant has given consent on the referral form or where the circumstances of the enquiry dictate this is necessary without consent);
- b) probation service;
- c) the Multi-Agency Risk Assessment Conference (MARAC);
- d) any other agency that can provide information to inform the risk assessment.

Scenario 2: the original applicant is C

56) Under Scenario 2, a DASH form should not be completed. Instead, the police should consider whether, subject to paragraphs 61-64 below, a decision to disclose information should be referred to the decision-making forum.

“Right to Know” entry route

Indirect information received by the police

- 57) For the purposes of the “right to know” entry route, the trigger which may lead to a disclosure under this scheme is where the police receive *indirect information* that may impact the safety of the victim (A) and which has not been conveyed to the police via the “right to ask” process.
- 58) “Indirect information” is likely to be information received by the police from intelligence-gathering arising from the following activities:
- a. an investigation into a criminal act where, as part of that investigation, the police have reason to believe that A may be at risk of harm from B;
 - b. information on alleged violent offending by B that is received from:
 - i. partner agencies (statutory and/or third sector) as part of routine information sharing at local safeguarding meetings;
 - ii. intelligence sources;
 - iii. either A or B coming into contact with the police as part of their routine operational duties.
- 59) Following receipt of the indirect information, minimum checks should be undertaken by the police to build an initial picture on A and B. The minimum standard of checks at this stage are:
- a. Police National Computer (PNC);
 - b. Police National Database (PND);
 - c. ViSOR (if the subject has a ViSOR marker on the Police National Computer);
 - d. local intelligence systems.

The National Intelligence Model should also be used to determine the veracity of the indirect information received.

- 60) To ensure that the safeguarding response is proportionate and in line with the risks identified, the police may prioritise which potential disclosures receive a full risk assessment under Stage 3. To assist in the process of prioritisation, consideration should be given to the following:
- a. whether A is judged to be at “high” or “medium” risk of harm from B;
- and/or
- b. whether A is associated with a serial perpetrator of domestic violence.

Referral to local decision-making forum

61) At this point in the Disclosure Scheme process it is envisaged that, from either the “right to ask” or “right to know” entry routes, sufficient information will have been gathered and checked to determine whether a credible risk of harm to A in the form of violent offending and/or behaviour from B exists. It will be for the local decision making forum to decide whether a disclosure should be made; however, before a referral is made to the local decision making forum, the police should categorise either the disclosure application (under “right to ask”) or the indirect information received (under “right to know”) as either a “concern” or “no concern”.

Categorising a “concern” or “no concern

62) 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:

a. B has convictions for an offence related to domestic violence (see annex A for list of offences) that may be disclosed under the terms of the Rehabilitation of Offenders Act 1974;

and/or

b. B is a serial perpetrator of domestic violence;

and/or

c. there is intelligence known about the previous violent offending of B which may include:

i. cases not proceeded with; and/or

ii. intelligence concerning violent offences; and/or

iii. previous concerning behaviour towards previous partners. This may include a pattern of behaviours that B has exercised coercive control over previous partners. *Note: the police may consider the impact of a spent conviction when conducting a risk assessment on A, regardless of the fact that the spent conviction can not then be disclosed.*

and/or

d. there is concerning behaviour by B demonstrated towards A. This may include a pattern of behaviours that indicate that B is exercising coercive control over A.

63) A ‘no concern’ applies where B has:

a. no convictions for an offence related to domestic violence that may be disclosed under the terms of the Rehabilitation of Offenders Act 1974;

and/or

b. there is no other intelligence that indicates that B’s behaviour may cause harm to A;

and/or

c. there is insufficient intelligence or information to register a concern.

64) This stage of the process should be reached no later than 5 working days from the face-to-face meeting (under “right to ask”) or from receipt of the indirect information (under “right to know”).

65) Once the police have determined whether the initial trigger can be categorised as a “concern” or “no concern”, the final decision to disclose must be referred to the local decision making forum for consideration at their next meeting. **It will be for the local decision making forum to make the final decision on whether the trigger is a “concern” or “no concern” based on the information gathered by the police and, consequently, whether a disclosure should be made.**

66) **If it is identified there is an immediate/imminent risk of harm to A, then ACTION MUST TAKEN IMMEDIATELY BY THE POLICE to safeguard those at risk.**

67) The local decision making forum should ideally be the Multi-agency Risk Assessment Conference (MARAC). If this is not possible, the decision making forum should be a multi-agency body which may consist of some or all of the following agencies:

- Police
- Probation Service
- Prison Service
- Health
- Housing
- Education
- Social Services
- Independent Domestic Violence Advocate (IDVA)
- A representative from each of the following:
 - women support service
 - victim support service
 - male support service
 - perpetrator programme

The minimum number of bodies constituting the local decision making forum should be no less than three, and consist of the police, probation service and IDVA.

68) The local decision making forum should consider the referral no later than 20 working days after the categorisation of the “concern” or “no concern” has been made by the police.

Principles the local decision making forum must consider when making a decision on whether to disclose

69) There are three principles that the local decision making forum must take into account before making the decision to disclose information that protects A.

Principle 1: Three-stage disclosure test

70) There is a general presumption that details about a person's previous convictions are confidential and, in such circumstances, the decision making form must ensure that the following 3 stage test is satisfied before a decision to disclose is made:

- a. that the local decision making forum has the power to disclose the information. As the police are relying on common law powers, then the police must be able to show that it is reasonable to conclude that such disclosure is necessary to protect the public from crime. In the context of this scheme, the police would have to conclude that disclosure to the applicant is necessary to protect A from being the victim of a crime;
- b. that there is a pressing need for such disclosure; and
- c. that interfering with the rights of B (as articulated in Article 8 of the European Convention of Human Rights, and Schedules 2 and 3 of the Data Protection Act 1998) to have information about his/her previous convictions kept confidential, is necessary and proportionate for the prevention of crime. This involves considering the consequences for B if his/her details 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.

- 71) 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 the police or other agencies to disclose to the applicant, the applicant may still be contacted to talk about the decision-making forum's concerns over the B's current behaviour. This discussion should cover 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 support A in the short, medium and long term, and determine the roles and responsibility of each agency to ensure that the safety plan remains victim-centred.

Principle 2: Data Protection Act 1998

- 72) Information about a person's previous convictions is also sensitive, personal data under the Data Protection Act 1998 and therefore the local decision making forum must also be satisfied that disclosure is in accordance with the eight principles set out in that Act (see Annex B for details of these principles and guidance on how they can be practically applied.)

Principle 3: Informing B of the disclosure

- 73) Consideration must also be given as to whether B should be told that information about him/her 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. Due consideration must be given on whether the disclosure to B would have potential to escalate the risk of harm to A. If this were to be the case, no disclosure must be given to B.
- 74) 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 Domestic Violence Disclosure Scheme and the implications for B. This also provides agencies with an opportunity to signpost B to relevant support services to allow B to address his/her offending behaviour.
- 75) Annex F contains a template checklist for the local decision making forum to refer to, which summarises the three principles articulated in this section of the guidance.

Decision made to disclose information

- 76) If the local decision-making forum makes a decision to disclose information because it judges that there is a risk of harm to A that warrants a disclosure, then the forum should consider the following points:

- a. what will be disclosed?

The forum will consider the specific wording of a 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.

- b. who should the disclosure be made to?

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 following the information gathered as part of this Disclosure Scheme process and subsequent risk assessments.

- c. how the disclosure should be made?

The forum will consider which agencies are best-placed to deliver the disclosure, based on the information at hand. It is good practice to consider a joint-agency approach to the disclosure provision.

It is strongly recommended that the disclosure should 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.

- 77) If disclosure is made, then the person receiving the disclosure must receive the following information:
- a) that the disclosure must only be used for the purpose for which it has been shared i.e. in order to safeguard A;
 - b) the person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose this information further;
 - c) 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.
- 78) If the person is not willing to sign the undertaking, the police 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.
- 79) At no time will written correspondence concerning the specifics of the disclosure consideration be sent out or left with the applicant in relation to the disclosure of information. There would be a potential risk to intelligence sources, victims and perpetrators should such written information get into the wrong hands. Annex G provides a template form which may be used to convey a disclosure. What the applicant is told should be recorded verbatim on this form, signed and then retained by the police. It must not be given to the applicant in any circumstances.
- 80) The person to whom the disclosure is made should be given information to empower them to safeguard A in the future. The contents of the information pack is at the discretion of the police but should as a minimum contain:
- a. Leaflet to explain Domestic Violence Disclosure Scheme
 - b. local leaflets that provide sign-posts to local support services

Decision made not to disclose information

- 81) If the local decision-making forum makes a decision not to disclose information because it judges that there is a no risk of harm to A that warrants a disclosure, then the forum should follow these actions:
- a. if the decision not to disclose has been made following the “right to know” entry point, 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.
 - b. if the decision not to disclose has been made following the “right to ask” entry point, then the following steps should be taken:
 - i. it is highly recommended that the applicant should be visited in person 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 given the information/details provided by the applicant and the result of checks made on these details.

- ii. However, it is important that the applicant is told that the lack of information to disclose this does not mean that there is no risk of harm to A, and the applicant should remain vigilant and report any future concerns. This contact also presents an opportunity to provide safeguarding information and signposting to relevant support services.
- iii. Annex H provides a template form which may be used to convey suitable wording.
- iv. the applicant should be given an information pack to help safeguard A in the future, but **at no time should the information pack contain written correspondence concerning the specifics of the disclosure consideration be sent out or left with the applicant in relation to the non-disclosure of information. There would be a potential risk of harm to A should such written information be obtained by a third party and/or B.**
- v. B will not be notified where no disclosure is made to the applicant.

Managing the perpetrator

- 82) Regardless of whether a decision is made to disclose information to safeguard A, the local decision making forum should also consider whether B should be referred to an appropriate local framework for managing offenders. Such a decision will be made based on the risk of harm posed by B's offending behaviour to the local community, and options may include referral either to the local:
- a. Multi-Agency Public Protection Arrangement (MAPPA)
 - or
 - b. Integrated Offender Management (IOM) scheme.
- 83) The local decision making forum should use the risk-assessment criteria in force by local MAPPA and IOM schemes to determine the appropriate scheme to which B might be referred.

Maintaining a record of the Disclosure Scheme

- 84) At the closure of every application (whatever the outcome and at any stage in the process) a final intelligence report must be submitted onto police and local agency intelligence systems to record the request, 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.
- 85) Any decisions made as a result of this scheme must be recorded fully and in a format that would stand scrutiny of any formal review including judicial review.
- 86) 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 under the heading *Principles underpinning the Domestic Violence Disclosure Scheme*.

Annex A – Non-exhaustive list of offences where convictions and/or allegations may be disclosed under the Domestic Violence Disclosure Scheme

The following list sets out the offences where a conviction or allegation may be disclosed under the Domestic Violence Disclosure Scheme. The list is non-exhaustive and is intended to act as a guide to the types of offences that may be disclosed.

- Battery
- Common assault
- Murder
- Manslaughter
- Kidnapping
- False imprisonment

- Under the Offences against the Person Act 1861:
 - section 4 (soliciting murder)
 - section 16 (threats to kill).
 - section 18 (wounding with intent to cause grievous bodily harm).
 - section 20 (malicious wounding).
 - section 21 (attempting to choke, suffocate or strangle in order to commit or assist in committing an indictable offence).
 - section 23 (maliciously administering poison etc. so as to endanger life or inflict grievous bodily harm).
 - section 28 (causing bodily injury by explosives).
 - section 29 (using explosives etc. with intent to do grievous bodily harm).
 - section 30 (placing explosives with intent to do bodily injury).
 - section 31 (setting spring guns etc. with intent to do grievous bodily harm).
 - section 35 (injuring persons by furious driving).
 - section 38 (assault with intent to resist arrest).
 - section 47 (assault occasioning actual bodily harm).

- Under the Public Order Act 1986
 - section 1 (riot).
 - section 2 (violent disorder).
 - section 3 (affray).
 - section 4 (fear or provocation of violence)
 - section 4A (intentional harassment, alarm or distress)
 - section 5 (harassment, alarm or distress)

- Under the Protection from Harassment Act 1997
 - section 2 (offence of harassment)
 - section 4 (putting people in fear of violence)

- Under the Explosive Substances Act 1883:
 - section 2 (causing explosion likely to endanger life or property).
 - section 3 (attempt to cause explosion, or making or keeping explosive with intent to endanger life or property).

- Under the Children and Young Persons Act 1933
 - section 1 (cruelty to children)

- Under the Firearms Act 1968
 - section 16 (possession of firearm with intent to endanger life)
 - section 16A (possession of firearm with intent to cause fear of violence)

- Under the Theft Act 1968:
 - section 7 (theft)
 - section 8 (robbery or assault with intent to rob)

- section 9 (burglary with intent to inflict grievous bodily harm)
 - section 10 (aggravated burglary)
 - section 21 (blackmail)
- Under the Criminal Damage Act 1971
 - section 1 (arson)
 - section 1(2) (destroying or damaging property) other than an offence of arson.
- Under the Criminal Law Act 1977
 - section 6 (violence for securing entry)
- Under the Criminal Attempts Act 1981
 - section 1 (attempting to commit an offence)
- Under the Child Abduction Act 1984
 - section 1 (offence of abduction of child by parent etc.)
 - section 2 (offence of abduction of child by other persons)
- Under the Criminal Justice and Public Order Act 1994
 - section 51 (intimidation, etc., of witnesses, jurors and others)
- Under the Crime and Disorder Act 1998
 - section 29 (racially or religiously aggravated assaults).
 - section 31 (racially or religiously aggravated public order offences)
 - section 31 (racially or religiously aggravated harassment)
- Under the Domestic Violence, Crime and Victims Act 2004
 - section 5 (causing or allowing the death of a child or vulnerable adult)
- Under the Sexual Offences Act 2003:
 - section 1 (rape).
 - section 2 (assault by penetration).
 - section 3 (sexual assault).
 - section 4 (causing a person to engage in sexual activity without consent).
 - section 5 (rape of a child under 13).
 - section 6 (assault of a child under 13 by penetration).
 - section 7 (sexual assault of a child under 13).
 - section 8 (causing or inciting a child under 13 to engage in sexual activity).
 - section 9 (sexual activity with a child).
 - section 10 (causing or inciting a child to engage in sexual activity).
 - section 11 (engaging in sexual activity in the presence of a child).
- Under the Asylum and Immigration (Treatment of Claimants etc.) Act 2004
 - section 4 (trafficking people for exploitation)

Annex B – 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:

1. 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.
2. 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.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. 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.
8. 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.

2. The Data Protection Act says that:

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 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 of, 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.

Annex C – Template of Minimum Standard of Information to be Obtained and Checks to be Completed at the Initial Contact Stage

(Unique reference number to be allocated to each enquiry and made reference to throughout the process)

Officer Recording:

Date:

Means of Contact:

Details of Applicant:

- Name (including any other names used, ie maiden):
- DOB:
- Place of birth:
- Address:
- Ethnic Origin:
- Gender:
- Preferred Language:

Preferred Method of Contact (Safety):

- Time:
- Day:
- Method:

Details of Subject:

- Name (including any other names used):
- DOB:
- Place of birth:
- Gender:
- Ethnic origin:
- Address including previous address(es):
- Place of work/employment:

Details of Person at Risk (if not applicant):

- Name (including any other names used):
- DOB:
- Place of birth:
- Gender:
- Ethnic origin:
- Address including previous address(es):
- Place of work/employment:

Details of Children:

- Name (including any other names used):
- Address:
- Ages (approximate if necessary):

Relationship:

- Nature of relationship between subject and person at risk:
- How would you describe the relationship:
- Length of relationship:

Concerns:

- What concerns have they in regard to the person at risk?:

Elements of Risk:

- Does the subject know that the enquiry has been made?:
- Concerns about subject knowing that you are making this application:

Information to be Read to Applicant:

- Does not replace existing procedures
- Disclosure will only be given to person at risk and/or person who is in a position to safeguard
- 24 hour timescale for checks to eliminate immediate risk
- Face-to-face meeting follows within 10 days
- Proof of ID required
- Enquiry will be completed within 35 days
- Do you consider yourself to be at risk from the subject?

Caveat: The person completing the forms has responsibility to complete all relevant checks, no disclosure at this stage (to be completed within 24 hours)

**If a crime is reported there is a duty to respond and conduct an investigation in line with normal operating procedures
(the Disclosure process will run alongside any investigation that is on-going)**

Annex D – Template for Initial Checks/Risk Assessment

This is the minimum standard of checks that are required at this initial contact stage. Any further checks that Forces feel are necessary are at their discretion. How these checks are to be recorded is to be decided by individual Forces.

Checks Completed on **Subject**:

- Officer recording:
- Date:
- PNC:
- PND:
- Intelligence check:
- DASH:

Checks Completed on **Applicant** (if not Person at Risk):

- PNC:
- Intelligence:

Checks Completed on **Person at Risk**:

- PNC:
- Intelligence:
- DASH:

**If a crime is reported there is a duty to respond and conduct an investigation in line with normal operating procedures
(the Disclosure process will run alongside any investigation that is on-going)**

Risk Assessment

Is there an Immediate or Imminent Risk of Harm Identified at this Stage?:

- **Yes** (immediate action to be taken to safeguard those at risk in line with standard procedures and record action below):

OR

- **No** (any relevant details to be recorded in making this decision):

Officer/Staff completing:

Date:

Additional Information:

Brief summary of information known at this stage, outcome of checks done and comments by Supervisors in support of decision made:

Annex E – Template for face-to-Face contact meeting

Minimum standard of information to be obtained and checks to be completed at the Face-to-Face stage

(Unique reference number to be allocated to each enquiry and reference to be made throughout the process)

Officer Recording:

Date:

Location:

Persons' Present:

Details of Applicant:

- Name:
- DOB:
- Place of birth:
- Address:
- Ethnic origin:

Verification of Identity (photographic identification required):

- Passport – number:
- Driving Licence – number:
- Birth Certificate:
- Other:

Further Details:

- Reason for contact and application?:
- Describe history of relationship:

Consent:

- Warning about providing false information
- Warning of further disclosing information received
- Name:
- Signature:
- Date:
- Officer Recording:
- Date:

Caveat: It is the responsibility of the person completing the form to conduct all relevant checks, no disclosure at this stage (although it seems unnecessary to repeat person's details and checks, it might be good practice to facilitate a tick box or guidance prompt to ensure none of the persons have come to notice since the initial contact check. At the discretion of Forces, further checks in regard to international enquiries could be warranted, CETS, etc).

Additional PND checks to be completed at this stage and consideration to the following:

Checks Completed on **Subject**:

- Officer recording:
- Date:
- PNC:
- PND:
- Intelligence check:
- DASH:

Checks Completed on **Applicant** (if not Person at Risk):

- PNC:
- Intelligence:

Checks Completed on **Person at Risk**:

- PNC:
- Intelligence:
- DASH:
- Are any immediate or imminent risk of harm factors identified at this stage? **(Action to safeguard to be taken at this stage as necessary)**

Annex F – Template checklist on disclosure decision making process by the local decision making forum

Section 1 – Questions for Consideration

- Is B known for domestic abuse related convictions?
- Where B is known for domestic abuse related convictions, does the Disclosure Application highlight safeguarding concerns in view of the nature of this previous history?
- Is B known for other offences relating to safeguarding (to include intelligence, breach of civil orders, harassment or injunctions, etc, Police National Database or information obtained by local checks)?

If B is known for offences/intelligence/information relevant to safeguarding and they are in an intimate relationship, give consideration to ‘concerns’ outcome route.

Reconsider if there is an immediate/imminent risk of harm identified and, if so, take immediate action to safeguard person(s) at risk.

Section 2 - Review the outcome of the initial contact and face-to-face stages

- Were concerns raised as a reason for making the application?
- Was the behaviour of the subject/applicant’s observations raised as a reason for making the application?

With all the above questions, consideration must be given as to why.

Reconsider if there is an immediate/imminent risk of harm identified and, if so, take immediate action to safeguard person(s) at risk.

Section 3 – Further Information

- Is there any other information, not covered in the above questions, that highlights safeguarding concerns.

If yes, give full details and consideration to ‘concerns’ outcome route.

CONCERNS: Yes / No (delete as applicable)

Rationale and justification for chosen outcome route (free text):

Officer/Agencies represented and completed:

DECISION: Disclosure / Non-Disclosure (delete as applicable)

CONSIDERATION GIVEN TO INFORM B OF DISCLOSURE:

Yes / No (delete as applicable)

Rationale and justification for chosen outcome route (free text):

Officer/Agencies represented and completed:

CONSIDERATION GIVEN TO REFER B TO APPROPRIATE LOCAL FRAMEWORK FOR MANAGING OFFENDERS (e.g. MAPPA, IOM)

Yes / No (delete as applicable)

Rationale and justification for chosen outcome route (free text):

Officer/Agencies represented and completed:

Section 4 – Legal Authority

- Due consideration be given to Common Law Power to disclose information about a person's convictions where there is a need for such disclosure to protect the public from crime;

AND

- Disclosure would not be in breach of the Human Rights Act 1998, Data Protection Act 1998 or a breach of confidence.

Annex G – Template containing minimum information to be disclosed (including form of words)

Template to be retained by the Police

Section 1 – Details of Person Receiving Disclosure Information

- Surname:
- Forename(s):
- DOB:
- Address:

Section 2 – Details of Subject of Disclosure Information

- Surname:
- Forename(s):
- DOB:

Section 3 – Details of Disclosure Meeting

- Time:
- Date:
- Agency:
- Persons present:
- Role:

Section 4 – Undertaking by Person Receiving Disclosure Information

The following information should be read as it appears below (verbatim) to the individual receiving disclosure information. If the individual does not agree to this undertaking, you should consider carefully whether disclosure should proceed at this point. **The decision to continue/to not continue must be considered prior to the actual visit and should be included in the risk assessment/decision making stage.** Also provide the individual with further contact details that can be accessed 24/7 in case there are further child protection concerns.

Prior to receiving any disclosure information you must clearly understand how you can use the information that is disclosed to you.

You can:

- use this information to keep yourself and others safe;
- use the information to keep your child(ren) safe;
- ask what support is available;
- ask who you should contact if you think you or others are at risk; and
- ask for advice on how to keep yourself and others safe.

You cannot:

- **share the information disclosed to you with any other person.** If you feel you need to share the information with another person, **you must contact the person or department who disclosed this information to you and seek their permission to do so.**

Failure by you to keep this information confidential may result in legal proceedings being instigated against you, depending on the circumstances.

You will be asked to sign an undertaking to agree to abide by the above and keep the information disclosed to you confidential. If you do not agree to sign this undertaking, it may result in you not receiving disclosure information.

UNDERTAKING

I understand the section above about how I can use the information disclosed to me in this meeting. I understand that the information is confidential and that legal proceedings against me may result if I breach this confidentiality. I agree to abide by these conditions in relation to the information that will be disclosed to me in this meeting:

Signature (of person receiving disclosure information):

Time:

Date:

Section 5 – Details of Disclosure of Information (NOT to be left with applicant in any format)

- Exact form of words being disclosed:

Section 6 – Declaration

I have received and fully understand the information that has been shared with me today. I understand the warnings I have been given about the confidentiality of this information.

Signature (of person receiving disclosure information):

Time:

Date:

Section 7 – Empowerment and Citizen-Focused Closure

An appropriate follow-on plan should be agreed for the person receiving disclosure. This should give consideration to what action the person should now be advised to take to safeguard their child(ren).

This should be explained to the person and the possible consequences of failure to follow this advice should be made clear.

Empowerment Pack issued or directed to website? Yes / No (delete as applicable)

The plan should note which agency is responsible for checking that the person follows advice to safeguard the child(ren) concerned; this may be the Police, Children’s Social Care or another appropriate agency. It should be noted which agency will provide any support to the person to assist with this; this may be the Police, Children’s Social Care or another appropriate agency/charity (eg Women’s Aid, Stop it Now!).

Any further queries or concerns contact:

Officer/Staff name:

Office No:

Department name:

24/7 Contact No:

Officer/Staff Making Disclosure

Officer/Staff completing:

Time:

Date:

Section Additional Information

Section No:

Details:

Annex H – Template form of words for non-disclosure

Template to be retained by police

Case Reference Number:

Dear (insert applicant's name):

The disclosure process provides a formal opportunity to contact the Police in order to make a request for information about a named individual who is in a relationship. In the event that this individual has convictions for domestic related matters careful consideration is given to disclosing information to a person at risk and or a person who is in a position to safeguard that individual. Disclosure may also be given where there is other information suggesting that the individual poses a risk of harm and disclosure is necessary to keep someone safe.

In relation to the enquiry that you made under the case reference number above, from the information that you provided to the Police and the checks made on these details, we can confirm that in line with criteria set out above, the Police have no information to disclose relating to the subject of your application.

Although there is no information to disclose to you on this occasion, you must remain vigilant to any indicators that this individual poses a risk of harm. The decision in this case is based on the information available to the Police service at this point in time. The Police will never be able to offer categorical assurances about the risk posed by any individual. Please refer to the Applicant Pack provided as part of the process for further information about safeguarding.

You are thanked for making a request under the Disclosure Process and we would take this opportunity to reiterate that your enquiry is a positive step towards keeping people safe.

If you have any further concerns in the future regarding for your safety or someone else you are encouraged to report your concerns to the Police or the Domestic Abuse Helpline on contact telephone numbers provided.

Signed:

Officer/Staff member:

Rank/Role:

Number:

Station/Department:

Date:

Local Police Telephone Number:

Domestic Abuse Helpline: