

Safety and justice: sharing personal information in the context of domestic violence – an overview

Patterns of Crime

Crime Reduction

Policing and Organised Crime

Criminal Justice System

Drugs and Alcohol

Offenders

Corrections

Immigration and Asylum

Social Cohesion and Civil Renewal

Economic Analysis and Modelling

Foreword

This Development and Practice Report comes with the full support and endorsement of the Inter-Ministerial Group on Domestic Violence. Issues concerning information-sharing by practitioners who encounter domestic violence came to Ministerial attention in a range of contexts. We recognised that meeting the needs of those who experience domestic violence can be a challenging and complex task and therefore sought to provide a concise, practitioner-focused tool to assist with this important work.

The report provides an introduction to responsible and lawful sharing of personal and sensitive information between practitioners in domestic violence contexts in England and Wales. The advance of ever-developing technology affords more opportunities for joined-up working than ever before. Practitioners are keen to develop their knowledge in information-sharing to take advantage of these new opportunities.

Historically, some practitioners may have been reluctant to share information due to a misplaced fear of falling foul of the legislative provisions. This report demonstrates that sharing personal and sensitive information can be done in a legal, pragmatic and straightforward way. The permissions and safeguards afforded by the current legal framework are outlined building on the lengthier and more complex guidance that is already available. The good practice case studies also ground the guidance in the everyday experience of practitioners working in 'front-line' contexts.

At its heart, this report keeps one principle central; the safety of domestic violence victims and their children must come first. Practitioners have long recognised that we must work together to do all that we can to remove the barriers preventing victims and their children getting the protection and support they need. Practitioners and agencies who do not communicate effectively can themselves be a barrier to this. Therefore, we recommend this report to all those practitioners in their various fields who are involved in providing the safe, quality, effective services that victims and their children need. Similar guidance will be issued in Northern Ireland which will take account of the different organisational and legislative situation there.

Rt. Hon. Baroness Scotland of Asthal QC
Home Office

Rt. Hon. Harriet Harman QC MP
Solicitor General

Lord Filkin CBE
Department for Constitutional Affairs

Baroness Ashton of Upholland
Department for Education and Skills

Melanie Johnson MP
Department of Health

Rt. Hon. Lord Rooker
Office of the Deputy Prime Minister

The Rt. Hon. Jacqui Smith MP
Department of Trade and Industry

Chris Pond MP
Department for Work and Pensions

Edwina Hart MBE AM
National Assembly for Wales

Angela Smith MP
Northern Ireland Office

This guide has been endorsed by the Inter-Ministerial Group on Domestic Violence

Safety and justice: sharing personal information in the context of domestic violence – an overview

Nicola Douglas, Sarah-Jane Lilley, Liz Kooper and Alana Diamond

The evidence base for this guide

This guide originates from the Home Office sponsored Crime Reduction Programme (CRP) Violence Against Women Initiative (VAWI). In 2000, 34 multi-agency, victim-focused pilot projects were funded and independently evaluated to identify 'what works' to support survivors and tackle domestic violence and rape and sexual assault. Five domestic violence projects from the initiative were selected as case studies. This aimed to explore the issues and barriers surrounding information-sharing and to highlight existing good practice. Three Data Protection Officers were interviewed and the Information Commissioner's Office was also consulted.

Introduction

Domestic violence (DV) accounts for around one-fifth of violent crime and claims the lives of two women every week (Simmons and Dodd, 2003). Research studies estimate that both women and children are abused in 30-60 per cent of cases (Mullender, 2000).

This guide aims to provide both agencies and practitioners with information and sources of further advice about how best to share information **lawfully** and **responsibly**.

What does this guide cover?

In this guide we aim to provide:

- A brief overview of why responsible information-sharing is so important in the context of DV, including how it benefits clients and the agencies that serve them.¹
- A brief introduction to the key legal provisions that relate to lawful information-sharing.²
- An introduction to good practice in information-sharing.

1. We have used various terms to refer to people experiencing or escaping DV for ease of comprehension. However, we appreciate that practitioners may prefer particular terms as appropriate to their working contexts.
2. Readers are advised that we do not aim to provide a full statement of the law and are directed to seek further information and expert advice where necessary.

- Sources of further information and advice, including guidance, toolkits and templates.

The guide draws upon examples from the CRP VAWI victim-focused projects (see evidence base above) and is balanced towards information-sharing concerning victims. However, the key principles also apply to the sharing of information about perpetrators.

Who is this guide for?

This guide is for practitioners who directly work with victims of domestic violence or are involved in the assessment of risk. The guide aims to inform decisions to share personal or sensitive information to protect victims and/or enable perpetrators to be brought to justice.³

This will include a range of professionals from the health, education, criminal justice and social welfare fields:

- GPs and other healthcare workers;
- teachers and other education staff;
- housing officers;
- social services staff;
- police and other criminal justice workers;
- NGO and voluntary sector workers.

3. A separate practitioner guide will be produced on sharing anonymised data for monitoring and evaluation purposes.

Home Office Development and Practice Reports draw out from research the messages for practice development, implementation and operation. They are intended as guidance for practitioners in specific fields. The recommendations explain how and why changes could be made, based on the findings from research, which would lead to better practice.

A multi-agency approach

It is now recognised that in order to meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs that individuals living with or escaping DV have, a **multi-agency partnership approach is required** (Hague, 2000; Humphreys, *et al*, 2001; Home Office, 2003).

The Crime and Disorder Act (1998) (CDA) places this obligation on a statutory footing, requiring some organisations to form partnerships to tackle crime and disorder, including DV, and provides a legal power to share information (Home Office, 1998).

A multi-agency partnership approach where the individual roles and joint responsibilities in relation to tackling DV and supporting victims have been clearly defined can enable partnerships to effectively address DV. The same principle of defined responsibilities applies to the sharing of information. Each agency must be aware of what information they can share with other agencies in the partnership and for what purpose. The development and agreement of information-sharing protocols enables the appropriate sharing of information (this will be fully discussed later in this guide).

Why share information?

Responsible information-sharing plays a key role in enabling organisations and professionals to protect DV victims and their children and to save lives.

Casework, advocacy, conducting risk assessments and providing general support and protection may all require information about individuals to be shared with other agencies.

Indeed, Articles 2 and 3 of the Human Rights Act (1998) (HRA) place an obligation on public authorities to protect people's right to life and their right to freedom from torture and inhuman and degrading treatment (see appendix 1). Meeting these obligations may necessitate lawful information-sharing.

The benefits of responsible information-sharing are detailed below. (See Box 1)

Box 1: Benefits to clients and their children

Responsible information-sharing enables:

- Timely action to be taken to protect clients and children from further abuse.
- Comprehensive risk identification and safety planning based on a full account of the facts and circumstances of each client's situation.

- The right sort and combination of advice, support and advocacy to be offered at the right time based on a full and accurate account of the client's needs and history, including other service contact and use.
- Clients to avoid the added distress of having to repeat details of their history or experience of DV and other circumstances each time they encounter a different service.

Benefits to agencies

Responsible information-sharing enables:

- Agencies to work together to protect DV victims and children in an informed and cohesive way.
- Duplication of effort to be avoided (e.g. in record taking, service provision etc.)
- Agencies to feel confident that they can provide a comprehensive, safe, quality service to clients, within the provisions of the law.
- Agencies to enhance their reputation for professionalism and credibility with clients and other agencies by demonstrating their competence in this area.

What is 'information'?

It is important to be clear about what is meant by 'information'. In this guide we are concerned with two types of information or data: 'personal data' and 'sensitive personal data'.⁴ (See Box 2)

Box 2: What is information? – Data Protection Act (1998) overview

- Personal data are: data which relate to a living individual who can be identified from that data or any other information held or likely to be held. It also includes any expression of opinion about the individual and any indications of the intentions of any person in respect of the individual.
- Sensitive personal data are: personal data which consist of information concerning racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical/mental health or condition, sexual life, alleged or committed offences, proceedings, disposal or sentence concerning any alleged or committed offences (Information Commissioner's Office (2001)).

The types of information agencies are likely to need to share to support victims, conduct risk assessments and help keep clients safe would be encompassed within these definitions, e.g. name and address, date of birth, number and age of children (personal data); details of historical and current abuse etc. (sensitive personal data).

4. Where we use the term 'information', we are referring to these two types of information unless otherwise specifically stated.

Responsible information-sharing – getting the balance right

Failing to share information (See Box 3) or doing so inappropriately (See Box 4) can put clients and their children at serious risk.

Box 3: Information-sharing – getting the balance right

In 1999, Mark Goddard was convicted of the murder of his wife Patricia after he stabbed her four times in the chest and abdomen. Patricia's post-mortem examination revealed 38 areas of previous injury and two areas of deep bruising to her scalp. In the five months before her death, her employer and six different agencies were aware of her problems and the abuse she was suffering including health, housing and police services. These agencies had never informed anyone else about their concerns. We cannot know if Patricia's life could have been saved but we do know that a far more comprehensive risk assessment could have been carried out if information had been disclosed to other agencies.

Box 4: Information-sharing – getting the balance right

In 1998, Gina McCarthy's husband had been refused contact with his baby son following their separation. The courts had ordered Gina to send her husband monthly progress reports via social services. Using the information from the monthly reports, Gina's husband identified Gina's home. He then traced Gina there and killed her in front of their son, whom he then abducted.

Professionals therefore need to work within the law, making pragmatic, case-by-case decisions, balancing the risks of information-sharing with the potential benefits of enhanced safety and protection for victims this might bring.

The final decision in any case will always depend on the particular circumstances involved and a system covering all eventualities is impossible to devise. However, using professional judgement backed by guidance, protocols and management/specialist advice where necessary professionals can be confident in carrying out this important duty of care to share information responsibly.

Training and awareness raising

Training for professionals for whom DV is not a specialism is also necessary to enable them to:

- raise their awareness about DV;
- examine and challenge the myths and stereotypes;
- recognise DV, including the 'symptoms' and consequences;
- confidently enquire about DV and respond competently to disclosures;

- identify the level of risk to the client and/or children;
- make informed decisions about when to share information, and when consent should be sought.

What is lawful information-sharing?

Confusion about the seemingly complex legal requirements can make professionals unsure how best to proceed. This guide does not intend to provide a detailed statement of the law on information-sharing. However, it does offer a simple and straightforward introduction to key considerations.⁵

Department for Constitutional Affairs information-sharing sequence

There is no single body of law that governs information-sharing. Instead, there is a legislative framework of gateways and protections.

To enable a public body to make a sound decision about whether to share information, the Department for Constitutional Affairs (DCA) advocates a straightforward 'sequence of consideration'.

Box 5: Sequence of consideration checklist (See also appendix 1)

If the answer to all these questions is 'yes' then lawful information-sharing may take place.	Yes
<i>Do you have a legal power to share information?</i> To share information lawfully, you must have the legal power (vires) to do so. For example, the Crime and Disorder Act 1998, Section 115 provides a legal power to share information for the purposes of the Act (i.e. crime prevention). This will apply in the majority of DV cases.	✓
<i>Are you in compliance with Article 8 of the European Convention on Human Rights (1998)?</i> The sharing of information by a public authority may not interfere with rights under Article 8 (which includes respect for private and family life, home and correspondence) unless it is in accordance with the law and 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 , the protection of health or morals, or the protection of the rights and freedoms of others .	✓

5. Readers are advised to seek further information and expert advice where necessary. See sources of further information and advice.

Are you in compliance with common law obligations of confidence?	✓
The common law requires that information may not lawfully be disclosed when given in certain circumstances of confidentiality (see appendix 1), unless certain exemptions apply. A key exemption concerns 'overriding public interest'.	
Are you in compliance with the Data Protection Act (1998)	✓
See below.	

In the following sections, we concentrate on the provisions of the DPA, as this was an area where practitioners most wanted clarification. However, it is important to emphasise the need to comply with the full range of legal requirements. In broad terms, this requires a legal basis to share information and compliance with the European Convention on Human Rights and common law obligations of confidence as well as the DPA. Further information on legal provisions is detailed in appendix 1 and in the DCA legal guidance (Department for Constitutional Affairs, 2003). Appendix 2 maps an information-sharing pathway as an example of the processes which all practitioners and agencies will need to consider.

The Data Protection Act (1998)

The Data Protection Act 1998 (DPA) is a key piece of legislation that regulates how information is processed.⁶ The DPA contains eight data protection principles, sometimes referred to as the 'principles for good information handling' that apply to all data shared about individuals and must be complied with (unless an exemption applies, see below).

Box 6: The eight data protection principles – an overview

Personal data must be:

1. Fairly and lawfully processed, (which includes the sharing of information).
2. Obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with those purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up to date where necessary.
5. Not kept for longer than necessary.
6. Processed in line with the data subject's rights.
7. Secure.
8. Not transferred to countries or territories 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 (Information Commissioner's Office, 2001).

6. The term 'processing' encompasses the disclosure of information to a third party.

Compliance with the schedule 2 and 3 conditions of the DPA is also vital when sharing information (see Box 7).

Box 7: DPA schedules 2 and 3 – conditions for processing personal/sensitive data

As part of compliance with the first principle of the DPA concerning fair and lawful processing (sharing of information):

- At least one condition from schedule 2 must be satisfied when processing personal data.
- Additionally, at least one condition from schedule 3 must be satisfied when processing sensitive data.

The schedule 2 and 3 conditions are outlined in appendix 3.

Processing data without consent according to the DPA

A consent-based approach to the sharing of information is the preferred practice in relation to victims (this is discussed below).

However, under the DPA, consent is only one of the schedule 2 and 3 conditions that will allow personal and sensitive data to be processed (shared).

There will always be situations and circumstances where there is a need to share information without consent in order to protect a client and/or any children, share information with specific agencies for risk assessment purposes or to bring perpetrators to justice.

Practitioners will need to make a careful assessment at the outset of their decision-making whether to set-aside the consent-based approach. This is because if consent is sought but refused it is not good practice to then share on a different basis (in effect, ignoring the earlier refusal of consent).

Instead, if the circumstances are such that there is a pressing need to share information in serious and justifiable circumstances that do not require a consent-based approach, it is advisable to pursue this from the outset, informing the data subject about the information-sharing.

We cannot provide for all of the specific circumstances where processing personal/sensitive data by relying on conditions other than consent may be necessary. However, three key contexts covered by the DPA that are likely to be relevant include:

➔ **Where the 'vital interests' of the client are at risk**

The Information Commissioner advises that this is where the sharing is necessary for matters of life and death or for the prevention of serious harm to the individual. We recommend that clear protocols and guidance must be in place to cover emergency circumstances such as this. (See appendix 3 for details of the 'vital interest' conditions.)

Box 8: A matter of life and death?

Instances of life and death decision-making to share information do occur. One case study project told us of a woman who had collapsed at the project; another recounted how a woman had telephoned a project worker immediately after taking pills in a suicide attempt. In both cases, an ambulance was called and relevant information disclosed. However, it is important to emphasise that the cases were treated individually on a case-by-case basis in clear and justifiable 'life and death' contexts.

➔ **Where processing is necessary for the purposes of 'administration of justice'**

This condition may equally apply to processing data about victims or perpetrators of DV. However, because consent is unlikely to be forthcoming from perpetrators, the 'administration of justice' provisions may be particularly applicable when processing data to bring perpetrators to justice. (See appendix 3 for details of the 'administration of justice' conditions.)

Box 9: An example of sharing information for 'administration of justice'

A woman reports a violent disturbance at her new home to the police. In her statement, she reports that her violent ex partner threatened her and smashed her windows, cutting his hands in the process.

The perpetrator has temporarily left the area but is arrested and charged when returning some weeks later. He denies the charges and alleges that the woman is making a malicious false accusation to harm his efforts to gain access to their children. During case review, the CPS requests that the police approach the hospital to check whether treatment was given for the cuts, which would corroborate the woman's evidence.

The hospital is part of a multi-agency partnership, which has a protocol for dealing with DV cases, including information-sharing. After careful consideration of medical confidentiality issues the hospital confirms having treated the perpetrator on the night of the incident.

➔ **Where processing is for public/statutory functions**

The DPA makes provision for processing which is necessary in the 'public interest'. The following case study is offered as an example of how this might apply.

Box 10: Protecting the public interest

A highly anxious young man telephones the Foreign & Commonwealth Office (FCO). His girlfriend has failed to return from a holiday to India with her family. He is afraid she is being held against her will to be forced into a marriage. He discloses that the young woman has had contact with social services, the police and a counsellor in the past. The young woman herself cannot be contacted. The FCO officer requests information from the professionals who have assisted in the past to help identify her whereabouts, assess the level of risk and inform officers overseas who may try to intervene.

In the case above, for example, the counsellor could consider processing the minimum amount of **personal data** that is necessary (e.g. known addresses, known contacts etc.) by relying on, schedule 2, 5(d). This allows processing which is necessary "...for the exercise of any other functions of a public nature exercised in the public interest by any person." However, there is no commensurate 'public interest' condition in schedule 3, and if wishing to process **personal sensitive data** another schedule 3 condition would need to be sought. Schedule 3 7(c) could apply which allows processing for "the exercise of any functions of...a government department" (in this case the FCO).

The police and social services could consider processing the minimum amount of **personal sensitive data** which is needed (e.g. information about previous abuse or threats from the young woman's family) under schedule 3, 7(b). This covers processing which is necessary for "... the exercise of functions conferred on any persons under enactment...". This includes statutory protective functions such as those held by police and social services.

In addition, there are other provisions within the DPA, introduced in 2000, which allow sensitive personal data to be processed (Stationery Office, 2000). However, readers should be aware that a considerably stronger case of public interest is required, which must be **substantial** in nature. (See appendix 3.)

Box 11: An example of substantial risk

An A&E nurse treats a woman who has been severely beaten by her partner. The nurse notes the woman has presented to A&E on a number of occasions over the last few months with injuries that were consistent with DV. The nurse conducts a DV risk assessment with the woman, which indicates that the future risk of her being severely abused or maybe even murdered is very high. However, the woman does not want to report the incident to the police nor does she want help from the local DV support project. The hospital is part of a multi-

agency partnership, which has a protocol for dealing with DV cases, and the sharing of information for risk assessment purposes. The nurse makes a decision based upon all the available information and shares the minimum amount of information with the police for risk assessment purposes only. This information can then be used by the police to inform their actions if called to respond to this individual in the future. The nurse informs the woman that the information has been shared with the police for risk assessment purposes and of the local DV support services available.

Using the crime and taxation exemptions in 'public interest' contexts

Section 29 of the DPA contains the 'crime and taxation exemptions'. These provisions include that where processing (sharing) is for the purpose of prevention or detection of crime, or the apprehension or prosecution of offenders, processing can be exempt from the 'non-disclosure provisions'. In practice the 'crime and taxation exemptions' may apply in the majority of DV cases that are criminal in nature, including the examples outlined in boxes 9, 10 and 11.

What does this mean? In basic terms, having satisfied a schedule 2 and a schedule 3 condition, the section 29 exemption removes the requirement that individuals are informed at the outset how their personal information will be used, who is responsible for it, how to contact them and who will have access to it.⁷

However, it must only be used on a case-by-case basis where there is 'substantial chance rather than a mere risk' that:

- i) not disclosing; or
- ii) informing the data subject of the intended disclosure would be likely to prejudice the prevention or detection of crime.

An obvious example where this might apply is where the police request information from the Benefits Agency about the whereabouts of a suspect. In broad terms, to comply with the principles of fair processing could in effect mean 'tipping-off' the suspect that the police are looking for him. The DPA recognises that to comply with the principles of fair processing in this case could obstruct the prevention/detection of crime and provides the Section 29 exemption to cover to situations such as this.

7. In strict terms, having satisfied a schedule 2 and 3 condition, this gives exemption from the first, second, third, fourth and fifth data protection principles when processing personal/sensitive data.

In summary, what the case studies most clearly illustrate is that the agencies concerned would need to assess how they can meet schedule 2 and 3 conditions and whether the crime and taxation exemptions apply to allow them to process the minimum amount of data which is necessary on a case-by-case basis. Consent, need not be the only condition relied upon and agencies will need to have in place protocols and guidance so that staff can confidently act when there is a need or intention to share information without consent for public interest purposes.

Processing for the purpose of child protection

It is well documented that DV is a risk factor for child abuse and vice versa (Humphreys, 2000). Recent legislation has further defined 'harm' to children to illustrate that this can include "impairment suffered from seeing or hearing the ill-treatment of another," for example, witnessing DV.⁸ (See appendix 1 Adoption and Children Act 2002)

It is beyond the scope of this document to provide detailed guidance on child protection matters. *Safeguarding Children. What To Do If You're Worried a Child is Being Abused* (Department of Health, 2003) contains a useful annex on information-sharing. In brief, this advises that practitioners must have due regard to the law surrounding information-sharing. However:

In general, the law will not prevent you from sharing information with other practitioners if:

- those likely to be affected consent; or
- the public interest in safeguarding the child's welfare overrides the need to keep the information confidential; or
- disclosure is required under a court order or other legal obligation (Department of Health, 2003).

The guidance offers advice to practitioners where there is a need to share confidential information to protect a child's welfare without consent. Relevant factors to consider include:

- What is the purpose of the disclosure?
- What is the nature and the extent of the information to be disclosed?
- To whom is the disclosure to be made (and is the recipient a relevant party under a duty to treat the material as confidential)?
- Is the proposed disclosure a proportionate response to the need to protect the welfare of a child to whom the confidential information relates?

8. The relevant provision of the ACA (section 120) will be implemented from January 2005.

Box 12: Keeping mothers informed where children are considered to be at risk

Where staff were concerned about potential harm to children in one case study project, they first discussed matters internally and then came to a decision about whether to inform social services and other appropriate organisations. A comprehensive child protection policy defined the terms within which disclosures could be made. Further good practice included sending a letter to inform guardians when decisions were taken to disclose without their consent detailing what would happen next, who would be contacted and when. This prioritised timely disclosure but kept guardians informed of concerns, issues and procedures.

The lawful basis for sharing information without consent where necessary concerning child protection is clear.

In summary, we have concentrated on the requirements of the DPA when sharing information without consent but it is worth re-emphasising that other legal and professional considerations will apply (see also appendix 1 on the common law of confidentiality for example).

Although in many cases, satisfaction of schedule 2 and 3 conditions will meet other legal requirements (e.g. 'public interest' concerns) professionals will need to satisfy themselves that this is the case.

Readers should therefore be aware of any specific codes of practice on information-sharing relevant to their profession. For example, medical professionals will be concerned to abide by the NHS Code of Practice on Confidentiality (see sources of further information and advice). Such codes detail the contexts within which information can be shared without consent.

In conclusion, there may be occasions when it is necessary to share information without consent; the duty of care and protection owed to clients may at times demand it. The DPA does not automatically prevent processing without consent and contains numerous provisions to allow for this.

A consent-based approach

However, as a matter of routine good practice professionals and agencies needing to share information should consider obtaining explicit written consent or documented verbal consent. There should not be a presumption that clients will not agree to their information being shared. A consent-based approach:

- provides the victim with a degree of control over any decisions, processes and their timing, in what is often a very dangerous situation;

- increases the likelihood of victims engaging with services, maintaining contact and re-contacting them in the future;
- increases the likelihood of victims accepting offers of advice, support and protection;
- gives professionals and organisations a strong form of protection against any future challenges.

The following scenario illustrates how professionals working together with the client's consent can help to expedite the solutions that clients and their children need.

Box 13: Sharing information with consent

A woman visits her GP who suspects she is being subjected to DV. Her GP has had recent training on encouraging and responding to disclosure of DV. With her consent, the GP refers the woman to the Women's Aid outreach worker, who attends the surgery. The outreach worker arranges emergency accommodation at a refuge. With her consent, the refuge shares information with the local housing department to assist with finding the woman and her children long-term, safe accommodation. In the case on which this scenario is based, the woman and her children were in their new home within three months.

What is consent?

The Information Commissioner provides the following definition of consent:

"Any freely given specific and informed indication of his (sic) wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Information Commissioner's Office, 2001, p.19).

Consent must be freely given and should not be:

- inferred;
- provided on the basis of misinformation or misleading statements;
- buried in small print or the implications otherwise disguised;
- provided under duress (Home Office, undated).

Opting in or opting out?

In the past, organisations may have inferred consent to information-sharing for administrative ease, operating an 'opt-out' system where clients had to signal their wish not to have their information shared. However, the DPA fair processing principles (principle one) requires that individuals are informed at the outset how their personal information will be used, who is responsible for it, how to contact them and who will have access to information.

Also, if relying on consent as a basis to share 'sensitive personal data' this must be 'explicit' and not inferred.⁹

Gaining explicit consent

According to DPA guidance, **explicit consent** must be "absolutely clear" and based on information provided about:

- the specific detail of the processing;
- the particular type of data to be processed (or even the specific information);
- the purposes of the processing;
- any other aspects of the processing that affect the individual, including disclosures that may be made of the data (Information Commissioner's Office, 2001, p.19-20).

Gaining explicit written consent need not be an onerous task and can be done as part of the routine process of initiating contact with clients.

Box 14: Gaining explicit consent – a routine approach

One DV case study project providing advice and advocacy services uses a standard form of words that they show to all clients before they ask them to sign a consent form. This is presented to the client and it is emphasised that this is all part of the usual process of enabling them to liaise on their behalf with other agencies to provide support. The project also ensures that clients are less likely to withdraw their consent by ongoing communication and reassurance that their data will only be used to help their situation in a positive way.

When seeking informed explicit consent from a client to share information the following checklist can be used.

- ✓ Has the client been informed of the reasons why her data may be shared?
- ✓ Has the client been informed of what information may be shared, when and with whom?
- ✓ Has the client been reasonably informed of the implications of her granting consent?
- ✓ Has the client been informed of her right to refuse consent, give partial consent (i.e. allow the sharing of some information) or withdraw it at any time?
- ✓ Have measures been put in place to ensure that the client will be kept up-to-date with the information-sharing process in relation to her information?

9. Home Office Circular 44/2001 also recommends that referrals of DV (and other specified) victims to Victim Support should follow positive 'opting-in' based on explicit consent (see sources of further information and advice.)

Clients may have additional needs due to learning difficulties, problems with reading and writing, sight or hearing impairments, lack of comprehension of English etc. Each client's needs should be assessed on an individual basis and additional steps taken such as the publication of information in a range of locally used languages, use of interpreters, and/or involvement of advocates and representatives to ensure that clients can give informed explicit consent. Such measures will be familiar to many agencies as part of their general provision of a client-centred and culturally sensitive service.

Gaining explicit verbal consent

In contexts where obtaining written consent is impracticable (e.g. telephone advice services) documented verbal consent can be obtained. (See Box 15.)

Box 15: Gaining documented verbal consent

In one case study project area a telephone helpline acts as a central referral point. Monitoring forms are used to record client details and clients are asked if they are willing for their details to be passed to the local DV support project. The decision of the client is then recorded in one of three check-boxes: 'Consent Given', 'Consent Denied', 'Consent Not Sought'. Any other advice or action taken is also recorded.

Where verbal consent is sought, the procedure should be evidenced and it is recommended that:

- a standard form of wording is used to request consent that covers the requirements of 'explicit' consent;
- the time, date and identity of the person seeking the consent are recorded;
- the decision of the client is recorded;
- relevant action such as any disclosure of information taken following the granting of consent is recorded.

Timing

In most cases, consent can be sought when clients come into contact with services. However, many frontline service providers encounter clients when they are emotionally distraught, confused and/or physically injured and it may not be possible or appropriate to obtain explicit consent to share information at this time. Professional judgement will come into play in making an assessment (Taket, forthcoming).

This issue may be particularly acute for 'front-line' police officers when attending incidents.¹⁰ Research for this guidance identified some good practice in agencies working together to clarify concerns and processes.

10. The Association of Chief Police Officers will be providing guidance to police officers on information-sharing in mid-2004.

Box 16: Obtaining consent at the scene of an incident

A DV support project worked extensively with local police to raise awareness about DV and the referral and support systems in place. Following training (covering the importance of referral, the need for written consent and methods for obtaining it) a protocol was agreed between the police and support agency. The police then began to provide victims with a card at the scene explaining the issues around giving consent; the reasons for seeking it and the agencies that the information would be shared with as part of the referral process. If granted, consent was recorded and relevant details were then passed to the support agency. Evidence suggests that this had a positive effect on police response to DV incidents and an increase in the recording of consent.

In 'front-line' contexts, timely decision-making about sharing information can be crucial to protecting victims. This guide recommends consideration of timing issues at a local level and clear guidance and training for professionals.

What to do if consent is refused

If a consent-based approach is initially pursued and consent is refused, practitioners should not, unless it is unavoidable, then seek to override this (for example by use of other schedule 2 and 3 conditions). In such circumstances expert advice should be sought.

If there is evidence to suggest there will be a need to share information without consent (for the reasons specified earlier) then it is good practice to pursue a non-consent approach from the outset. This makes it especially important for practitioners to make a careful assessment at the outset whether consent should be sought or whether the circumstances are such that the consent-based approach needs to be set aside.

A note on documentation

Good documentation prevents clients from having to recount their circumstances repetitively; helps to protect professionals in the unlikely event of legal challenge and provides evidence of abuse should the client wish to pursue a legal case against the perpetrator. As a minimum, documentation might include:

- relevant personal details such as name, address, age and details concerning any children;
- pertinent facts about the abuse suffered;
- the granting (or withholding) of consent to share information;
- decisions and actions taken by the professional concerned;

- the grounds for sharing any information with other professionals or agencies;
- any follow-up information that a professional taking over the case would need to know.

Working in partnership

A partnership approach where the individual roles and joint responsibilities and accountabilities have been clearly defined in a [written agreement or protocol](#) provides the best way to ensure that information-sharing is done safely, lawfully and effectively. (See appendix 4 for a suggested process for this.)

What should a protocol contain?

Local needs and requirements mean that we cannot provide an exhaustive list of what a protocol should cover. However, Box 17 outlines key information that a protocol might usefully contain.¹¹

Box 17: Suggested components of an information-sharing protocol

- A list of the parties to whom the protocol applies (and rights to withdraw).
- The lawful basis under which parties will share information (e.g. Crime and Disorder Act 1998, section 115), and other relevant laws requiring compliance (e.g. Human Rights Act 1998, common law on confidentiality, Data Protection Act 1998, Children Act 1989 etc.).
- The purpose of the agreement (e.g. to enable lawful information-sharing between agencies for the purpose of preventing repeat DV victimisation and holding offenders to account).
- Agreed definitions of DV and any other important terminology.
- The circumstances and processes for permitted disclosures (e.g. child protection concerns, DV service referral, case tracking etc.).
- Arrangements and accountabilities for the collection, storage, processing and disclosure of information within the terms of the law and the protocol.
- How the rights of 'data subjects' will be upheld (including access to information, corrections, amendments and complaints).
- Steps to be taken following allegation of breach of the agreement.
- Accountabilities and timescales for review of the protocol.
- Arrangements for personal data held when parties withdraw from the agreement.

11. See sources of further information and advice for details of the DCA and Home Office information-sharing websites where examples and guidance on developing a protocol can be obtained.

Safe storage

Partners will also wish to negotiate the practical considerations of safe storage of any information shared. DPA principle seven requires that information is held securely (see Box 6). "Reasonable steps" must be taken to ensure the reliability of staff having access to data and consideration must be given to the **nature of the data to be protected** and the **harm that might result from a breach of security**. These are crucial considerations in DV cases where the safety of the client and any children must be kept central to the process.

The Information Commissioner advises that standard risk assessment and management techniques will often be sufficient to:

- (a) identify potential threats to the system;
- (b) identify the vulnerability of the system to those threats;
- (c) design counter measures to reduce and manage the risk (Information Commissioner's Office, 2001, p.27).

Conclusions

It is only by working in partnership that we can hope to realise our aim of bringing prevention, protection, justice and support to the survivors of DV and their children, and holding the perpetrators to account. Good information-sharing has an integral and essential role to play, and as this guide has shown, it is possible to share information to both protect and support survivors in a straightforward and efficient way with the full support of the law.

Acknowledgements

We would like to thank the CRP VAWI domestic violence projects and local Data Protection Officers who assisted by sharing case studies and good practice examples to inform this report.

We are also grateful to the following colleagues for their invaluable expert advice and assistance: members of the Cross-Governmental Unit on Domestic Violence; D.I. Joyce Green (Lancashire Constabulary); Sue Bridge (Cheshire Domestic Abuse Partnership); Beryl Foster (Standing Together); Chris Walker, Rocío Ferro, Jennifer Flaschner, Paul Boyle & Hannah Lockley (DCA); Chris Blairs, Emma Churchill, Gwyn Jones, Sarah Getgood, Suzanna Lyle & David Noble (Home Office); Kussum Sharma, Peter Clarke, David Evans, David Smith & Richard Thomas, (Information Commissioner's Office); Dr. Kate Paradine (Centrex); Dr. Susan Edwards (University of Buckingham); Prof. Ann Taket (London Southbank University); Prof. Audrey Mullender (University of Warwick); Debbie Crisp (Consultant).

Sources of further information and advice

Information helplines

Office of the Information Commissioner information line:
01625 545 745

Home Office Information-sharing helpline:
020 7273 4015

Key websites

The Information Commissioner's Office website provides detailed information on all aspects of information-sharing, including:

- legal advice and guidance for both the public and private sectors;
- an audit guide to enable an assessment of compliance with the DPA;
- codes of practice;
- contact details for their enquiries services.

<http://www.informationcommissioner.gov.uk/>

Home Office Crime Reduction Information-sharing 'Minisite' includes:

- an information-sharing toolkit;
- legal advice;
- interactive protocol template 'wizard';
- information-sharing network details;
- contact details for their enquiries services.

<http://www.crimereduction.gov.uk/infosharing00.htm>

The Department for Constitutional Affairs Information-sharing website includes:

- an information-sharing toolkit;
- legal guidance;
- guidance on complaints procedures;
- a library of protocols from the health and social care, child protection and crime prevention sectors.

www.dca.gov.uk/foi/sharing/index.htm

Other useful documents and briefings

NACRO Briefing: Making It Count – A Practical Guide to Collecting and Managing Domestic Violence Data.
<http://www.nacro.org.uk/templates/publications/briefingItem.cfm/2003080700-csps.htm>

Youth Justice Board and ACPO publication: Sharing Personal and Sensitive Information in Respect of Young People at Risk of Offending. A Practical Guide.

<http://www.youth-justice-board.gov.uk/YouthJusticeBoard/AboutUs/News/NewsArchive/InfoSharing.htm>

Department of Health Guidance: What to Do If You Are Worried a Child is Being Abused - Information-sharing Guidance Annex.

<http://www.publications.doh.gov.uk/safeguardingchildren/>

Department for Education and Skills. Identification, Referral and Tracking Initiative. Information-sharing to Improve Services for Children Guidance.

<http://www.cypu.gov.uk/corporate/publications.cfm>

NHS Confidentiality Code of Practice.

http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4069253&chk=jftKB%2B

NHS 12 Key Points on Consent.

http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4006131&chk=DCfGrJ

[General Medical Council](#) Guidance on Patient Confidentiality.

<http://www.gmc-uk.org/standards/secret.htm>

[Home Office Circular 44/2001](#): Referral of Victims' Details to Victim Support/Revised Version of 'Victims of Crime' Leaflet

<http://www.homeoffice.gov.uk/docs/hoc44.html>

[ACPO Position Statement](#) – Public Protection, Multi-Agency Working and Information-sharing (forthcoming)

[NHS Scotland Computer Based Learning Pack on Data Protection](#)

<http://www.show.scot.nhs.uk/elearning/>

[Department of Trade and Industry](#). Hard Facts – Information Security and Why You Need It

http://www.cst.gov.uk/industries/information_security/downloads.html

[Department for Work and Pensions](#) data protection publications, including how to obtain: Data Sharing of Personal Information (see Data Protection section)

http://www.dwp.gov.uk/pub_scheme/classes/operatio.asp

[Welsh Assembly Circular: Guidance On Protocols For Sharing Information](#) (NAFWC 22/2003 WHC, 2003, 50)

<http://www.wales.gov.uk/keypubliclegislationcirculars/index.htm>

Sources of advice and support for DV victims and advocates

[National 24 hour Domestic Violence Helpline](#) A service run in partnership by Women's Aid and Refuge.

0808 2000 247 (minicom available)

http://www.womensaid.org.uk/help/national_helpline.htm

Refuge

020 7395 7700

<http://www.refuge.org.uk/>

Women's Aid

0117 944 4411

<http://www.womensaid.org.uk/>

Welsh Women's Aid

029 20 39 0874

<http://www.welshwomensaid.org/>

[BAWSO](#) (Welsh organisation for Black women who are victims of domestic violence)

029 2043 7390

[Southall Black Sisters](#) (Advice and support for women from Black and minority ethnic communities)

020 8571 9595

[Broken Rainbow](#) (Pan-London Lesbian, Gay, Bisexual And Transgender Domestic Violence Forum)

0781 2644914

<http://www.lgbt-dv.org/html/rainbow.htm>

Victim Support

0845 30 30 900

<http://www.victimsupport.org.uk/>

[CJOnline website](#) (Contains an interactive virtual tour to provide information about the criminal justice system process as it relates to victims of crime)

<http://www.cjonline.org/citizen/victims.html>

National Child Protection Helpline (NSPCC)

0800 800 500

<https://www.nspcc.org.uk/nspcc/helpline>

The Samaritans

08457 90 90 90

<http://www.samaritans.org/>**Shelterline** – National 24-hour Housing Helpline

0808 800 4444

<http://www.shelter.org.uk/housingadvice/shelterline/index.asp>**Careline** (Counselling services)

020 8514 1177

Community Legal Service Directory Line

0845 608 1122

<http://www.justask.org.uk/index.jsp>**Office of the Deputy Prime Minister** Information and guidance on funding for domestic violence services via the Supporting People Programmewww.spkweb.org.ukhttp://www.odpm.gov.uk/stellent/groups/odpm_homelessness/documents/page/odpm_home_601544.hcsp**Foreign & Commonwealth Office** (Advice on forced marriage)

020 7008 0135/0230

Reunite (UK charity specialising in international parental child abduction)

0116 2556 234

<http://www.reunite.org/>**References**

Department for Constitutional Affairs (2003) *Public Sector Data Sharing: Guidance on the Law*. London: Department for Constitutional Affairs.

Department of Health (2003) *What to Do if You're Worried a Child Is Being Abused*. London: Department of Health.

Hague, G. (2000) *Reducing Domestic Violence...What Works? Multi-Agency Fora*. One of a pack of 12 briefing notes, Crime Reduction Research Series No. 4. London: Home Office. <http://www.homeoffice.gov.uk/rds/crimreducpubs1.html>

Home Office Crime Reduction Programme Toolkit on Using Intelligence and Information (undated)

<http://www.crimereduction.gov.uk/toolkits/ui00.htm>

Home Office Crime and Disorder Act Introductory Guide (1998) <http://www.homeoffice.gov.uk/docs/cdaint1.html>

Home Office (2003) *Safety and Justice: The Government's Proposals on Domestic Violence*. London: The Stationery Office.

Humphreys, C. (2000) *Child Protection and Woman Protection: Links and Schisms. An Overview of the Research*. Women's Aid Website. <http://www.womensaid.org.uk/campaigns&research/research/child%20protection.htm>

Humphreys C., Hague, G., Hester, M., Mullender, A. (2001) *Domestic Violence Good Practice Indicators*. Centre for Study of Safety and Well-Being. Warwickshire: University of Warwick.

Information Commissioner's Office (2001) *The Data Protection Act 1998. Legal Guidance*. Information Commissioner's Office.

Mullender, A. (2000) *Reducing Domestic Violence...What Works? Meeting the Needs of Children*. One of a pack of 12 briefing notes, Crime Reduction Research Series No. 4. London: Home Office. <http://www.homeoffice.gov.uk/rds/crimreducpubs1.html>

Simmons, J. and Dodd, T. (2003) *Crime in England and Wales 2002/2003*. Home Office Statistical Bulletin 07/03. London: Home Office. <http://www.homeoffice.gov.uk/rds/hosbpubs1.html>

Stationery Office (2000) Data Protection Processing of Sensitive Data Order, S.I. 2000/417

<http://www.hmso.gov.uk/si/si2000/20000417.htm>

Taket, A. *Tackling Domestic Violence: The Role of Health Professionals*. London: Home Office (forthcoming).

Appendix 1: Overview of legal provisions relating to information-sharing

N.B. This is not a full statement of the law. Readers are advised to seek further information and expert advice where necessary.

The least you need to know

Data Protection Act 1998 (DPA)

The DPA safeguards individual rights and regulates the processing of 'data' and 'sensitive personal data' in electronic and some manual forms giving guidance on obtaining, storing and the use and disclosure of information about individuals.

- The Act details the rights of individuals to access data held about them (known as 'subject access') and the need for data controllers to notify the Information Commissioner (subject to exemptions), with penalties for failing to do so.
- Contains eight data protection principles (subject to exemptions, see below), which must be complied with by those who 'control' data (See Box 6).
- See Box 7 and appendix 3 of this guide concerning the conditions for processing 'personal data' and 'personal sensitive data'.
- Section 29 (known as the 'crime and taxation' exemptions) regards data processed for the prevention or detection of crime and/or the apprehension or prosecution of offenders. However, Section 29 does not exempt from the requirement to comply with schedules 2 and 3 concerning processing personal/sensitive data. The Information Commissioner has stated that where relying on these exemptions, there would need to be a substantial chance, rather than a mere risk that in the particular case the purposes (e.g. detection/prevention of crime, apprehension/prosecution of offenders) would be noticeably damaged by failure to process. Moreover, the exemptions should not be used for routine processing and should be considered on a 'case-by-case' basis. If challenged, the data controller must be prepared to defend their decision to act under the exemptions to the Commissioner or the Courts and that it is advisable for each decision to do so to be taken at a senior level, with reasons documented.¹

The Crime and Disorder Act 1998 (CDA)

The CDA aims to tackle crime and disorder and help create safer communities.

- Section 115 of the CDA provides a power (but not an obligation) for information sharing between 'responsible' public bodies (e.g. police, local authority, health authority) and with 'co-operating' bodies (e.g. DV support group, victim support group) participating in the formation and implementation of the local crime and disorder strategy. This must be to pursue a specific objective within the strategy and be subject to a written agreement.

1. Information Commissioner's Office (2002) The Data Protection Act. A Brief Guide for Data Controllers. Information Commissioner's Office.

Further Information (See also sources of further information and advice)

➔ Link to the Act

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm#aoifs>

➔ Link to Data Protection (Processing of Sensitive Data Order) 2000. <http://www.hmso.gov.uk/si/si2000/20000417.htm>

➔ Information Commissioner's Legal Guidance

<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>

➔ Department for Constitutional Affairs Public Sector Data

Sharing Legal Guidance

<http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf>

➔ NHS Scotland Computer Based Learning Pack on Data

Protection <http://www.show.scot.nhs.uk/elearning/>

➔ Link to the Act

<http://www.hmso.gov.uk/acts/acts1998/19980037.htm#aoifs>

➔ Home Office Crime and Disorder Act Introductory Guide

<http://www.homeoffice.gov.uk/docs/cdaaint1.html>

➔ Information Commissioner's Guidance on the Act

<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>

<ul style="list-style-type: none"> ● In addition, Section 115 stipulates that any person who would not have power to disclose information to a relevant authority or a person acting on behalf of such an authority shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of the Act. ● This power must be exercised in accordance with any other relevant legislation, including the HRA, common law of confidence and the DPA. 	<p>→ Department for Constitutional Affairs Public Sector Data Sharing Legal Guidance http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf</p>
<p>The Human Rights Act 1998 (HRA) (which gives force to the European Convention on Human Rights, ECHR) <i>The ECHR contains fundamental rights and freedoms such as the right to life, the right to a fair trial and freedom of thought, religion and speech and respect for private and family life.</i></p> <ul style="list-style-type: none"> ● Article 2.1 stipulates that "Everyone's right to life shall be protected by law". ● Article 3 stipulates that 'No one shall be subjected to torture or to inhuman or degrading treatment or punishment'. ● Article 6 stipulates the right to a fair trial. ● Article 8.1 stipulates that "Everyone shall have the right to respect for his private and family life, his home and correspondence... There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is 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". 	<p>→ Link to the Act http://www.hmsso.gov.uk/acts/acts1998/19980042.htm</p> <p>→ Department for Constitutional Affairs Public Sector Data Sharing Legal Guidance http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf</p> <p>→ Crime Reduction Programme Guidance on the Act http://www.crimereduction.gov.uk/hra.htm</p>
<p>The Children Act 1989 (CA) <i>The CA redefined the law around child welfare and introduced new measures for working with children and families.</i></p> <p>Key principles include:</p> <ul style="list-style-type: none"> ● The child's welfare is paramount. ● Professionals will work in partnership with the child, with other professionals and with the parents and significant others. ● Section 27 stipulates that where it appears to a local authority that any authority or other person mentioned in subsection (3) (see below) could, by taking any specified action, help in the exercise of any of their functions under this part, they may request the help of that other authority or person, specifying the action in question. An authority whose help is so requested shall comply with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions. <p>Agencies listed in subsection 3 are:</p> <ol style="list-style-type: none"> (a) any local authority; (b) any local education authority; 	<p>→ Link to the Act http://www.hmsso.gov.uk/acts/acts1989/Ulkpqa_19890041_en_1.htm#tcon</p> <p>→ Department of Health Working Together to Safeguard Children Guidance http://www.doh.gov.uk/quality5.htm</p> <p>→ Department of Health. What to Do If You Are Worried a Child is Being Abused – Includes Annex on Information Sharing http://www.publications.doh.gov.uk/safeguardingchildren/</p> <p>→ Department of Health. Identification, Referral and Tracking Initiative. Information Sharing to Improve Services for Children Guidance www.cypu.gov.uk/corporate/docs/IRTGuidance%20v%20%208%2005-02%20doc.pdf</p>

<p>(c) any local housing authority; (d) any health authority; and (e) any person authorised by the Secretary of State for the purposes of this section.</p> <ul style="list-style-type: none"> Section 47 places a duty on the above authorities to assist with enquiries (in particular by providing relevant information and advice) if called upon by the authority conducting enquiries following reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm. 	<p>→ Link to the Act http://www.hmso.gov.uk/acts/acts2002/20038-i.htm#120 → For details of how to obtain the Department of Health guidance http://www.children.doh.gov.uk/adoption/law.htm</p>
<p>Adoption and Children Act 2002 (ACA)</p> <p><i>The ACA modernises the law on adoption in line with the Children Act 1989.</i></p> <ul style="list-style-type: none"> Section 120 amends Section 31(9) of the Children Act 1989 to extend the definition of harm to include "impairment suffered from seeing or hearing the ill-treatment of another". The relevant provision of the ADC (section 120) will be implemented from January 2005. 	<p>→ NHS Confidentiality Code of Practice http://www.ch.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/Article/fs/en?CONTENT_ID=40692538&chk=jfkB%2B → NHS 12 Key Points on Consent http://www.ch.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/Article/fs/en?CONTENT_ID=4006131&chk=DCfGrJ → Information Commissioner's Guidance of Use and Disclosure of Health Data http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5ca6def30802566360045bf4d/7b7d02d29c28e76d802566bb5005d7bb3</p>
<p>Common law relating to confidentiality</p> <p><i>The common law protects from disclosure of information (whether personal or not) given in 'confidential' contexts.</i></p> <ul style="list-style-type: none"> Breach of confidence may be demonstrated where the information: <ul style="list-style-type: none"> Has a 'quality of confidence' (i.e. should not already be in the public domain and has sensitivity and value); Is given in circumstances giving rise to an 'obligation of confidence' on the part of the person to whom the information has been given (e.g. nurse/patient); Is used in a way that was not authorised.² However, the duty of confidentiality is not absolute. Disclosure can be justified if: <ul style="list-style-type: none"> The information is not confidential in nature; The person to whom the duty is owed has consented to the disclosure; There is an overriding public interest in disclosure; Disclosure is required by a court order or other legal obligation.³ 	<p>→ General Medical Council Guidance on Patient Confidentiality http://www.gmc-uk.org/standards/secret.htm → Department for Constitutional Affairs Public Sector Data Sharing Legal Guidance http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf</p>

2. Department for Constitutional Affairs (2003) Public Sector Data Sharing: Guidance on the Law. London: Department for Constitutional Affairs.
 3. Department of Health (2003) What to Do if You're Worried a Child Is Being Abused. London: Department of Health.

Freedom of Information Act 2000 (FOI)

The FOI enables any member of the public to apply for access to information held by bodies across the public sector. The legislation will apply to a wide range of public authorities, local authorities, health trusts, doctors' surgeries and other public organisations. Comes into full force in 2005.

- The Act provides a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions. Alongside other legal protections, the exemptions provide grounds for refusal to provide information. This could include a request made under the Act about DV survivors by alleged perpetrators. Sections 22-44 contain the exemptions, which include:
 - Where held in the investigation, prevention, detection or prosecution of a crime or the apprehension of offenders or the administration of justice.
 - Where held as court documentation.
 - Where disclosure would constitute a breach of confidence.
 - Where legal professional privilege exists.

→ Link to the Act

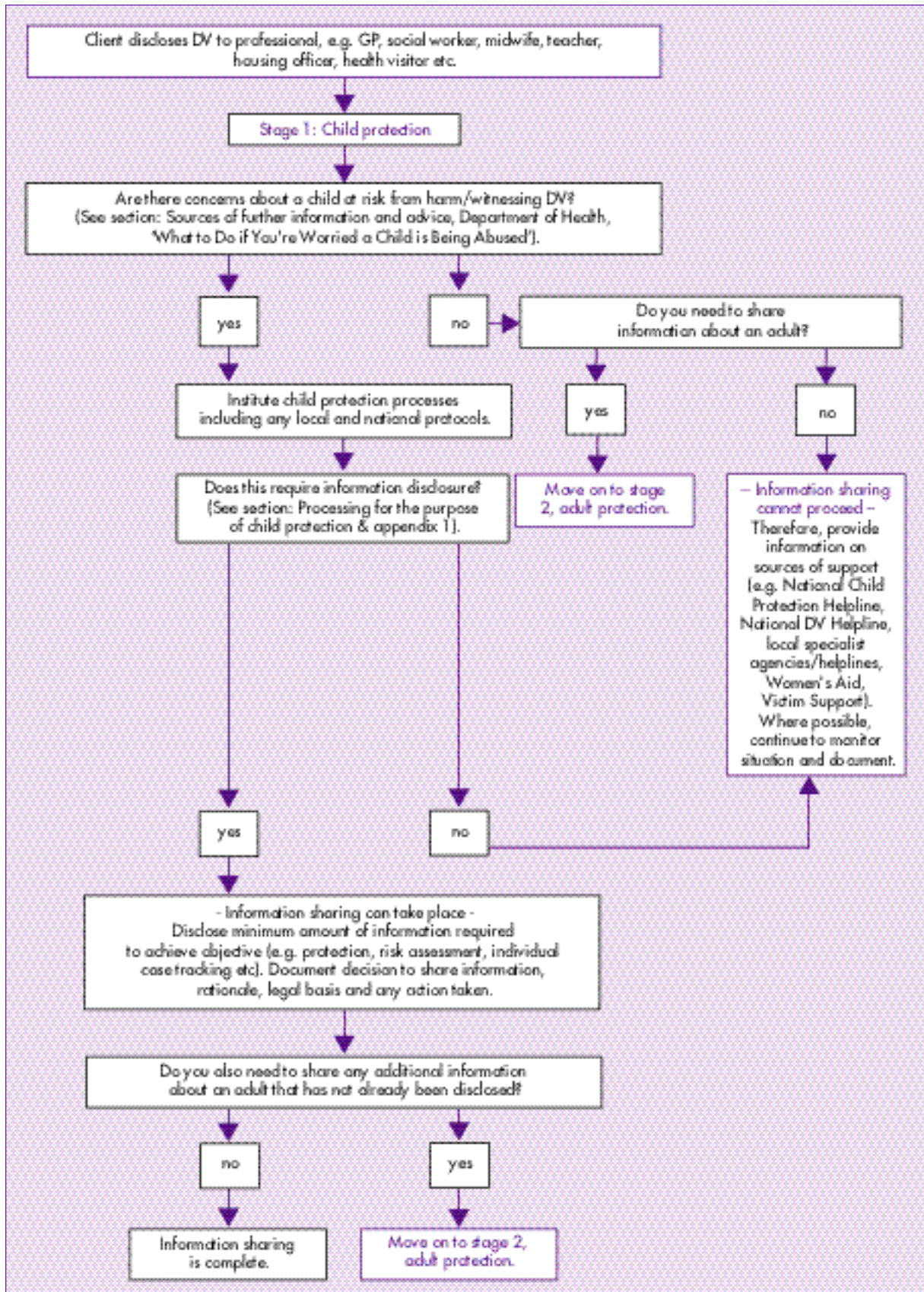
<http://www.hmsa.gov.uk/acts/acts2000/20000036.htm>

→ Information Commissioner's Guidance on the Act

<http://www.dataprotection.gov.uk/dpr/foi.nsf>

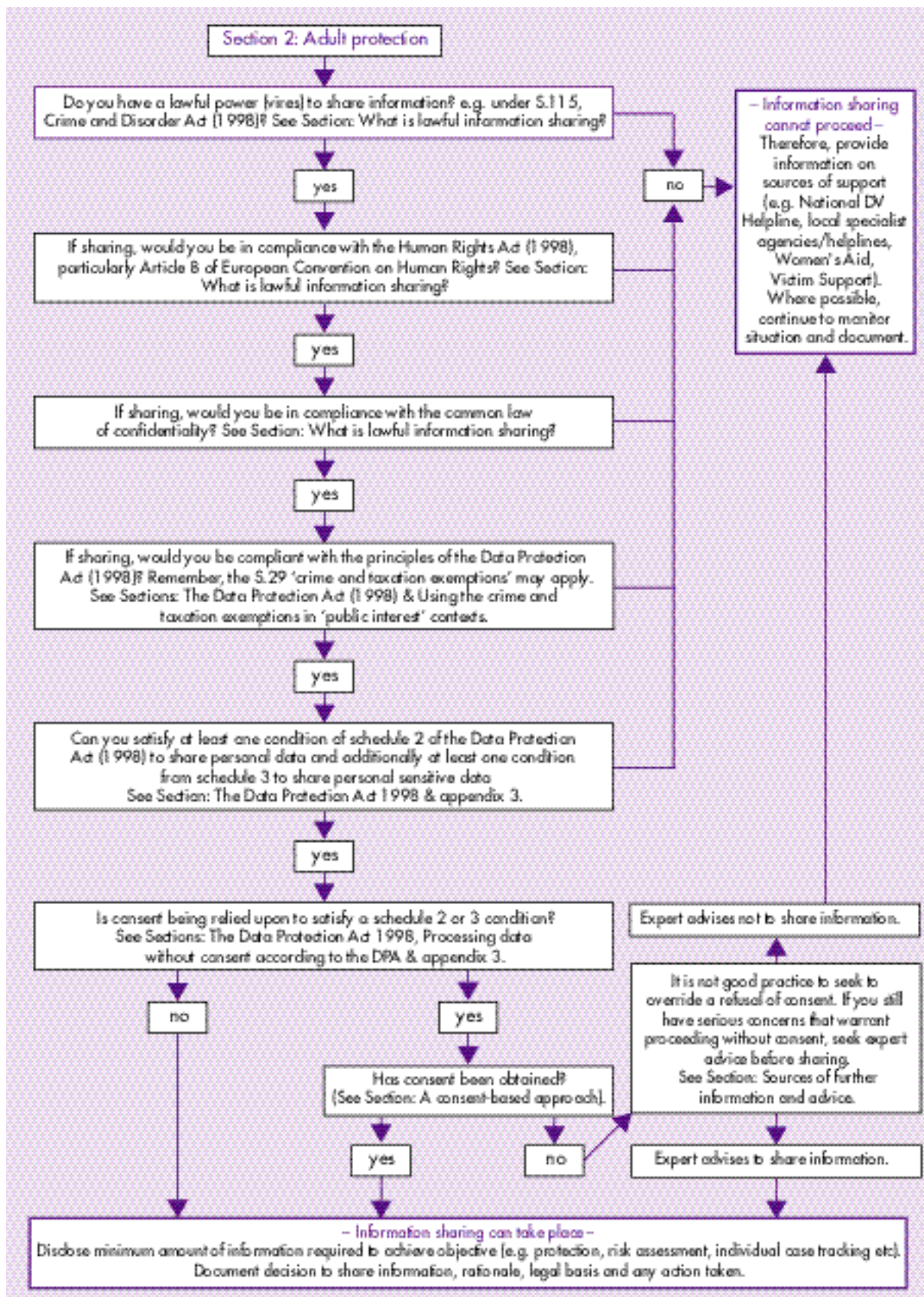
Appendix 2: Example of an information-sharing pathway (stage 1) – child protection

It is good practice for professionals to receive training, which aims to increase their awareness of child abuse and DV; examine the myths and stereotypes; confidently enquire about child abuse and DV; identify the level of risk to the client and any children and to respond effectively to disclosures.



Appendix 2: Example of an information-sharing pathway (stage 2) – adult protection

It is good practice for professionals to receive training, which aims to increase their awareness of DV; examine the myths and stereotypes; confidently enquire about DV; identify the level of risk to the client and to respond effectively to disclosures.



Appendix 3: Summary of conditions in schedules 2 and 3 of the Data Protection Act 1998

Adapted from 'Public Sector Data Sharing, Guidance on the Law' – Department for Constitutional Affairs, 2003

Conditions in schedule 2 relating to the processing/sharing of personal information/data

Paragraph 1: The data subject has given consent to the processing.

Paragraph 2: The processing is necessary for (a) the performance of any contract to which the data subject is a party; or (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

Paragraph 3: The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

Paragraph 4: The processing is necessary in order to protect the vital interests of the data subject.

Paragraph 5: The processing is necessary: (a) for the administration of justice; (b) for the exercise of any functions conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or government department; or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

Paragraph 6(1): The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Paragraph 6(2): The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Conditions in schedule 3 relating to the processing/sharing of sensitive information/data

Paragraph 1: The data subject has given explicit consent to the processing.

Paragraph 2: The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.

Paragraph 3: The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained.

Paragraph 4: The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit body.

Paragraph 5: The processing is of information made public as a result of steps deliberately taken by the data subject.

Paragraph 6: The processing is necessary in connection with legal proceedings or legal advice.

Paragraph 7: The processing is necessary (a) for the administration of justice; (b) for the exercise of any function conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

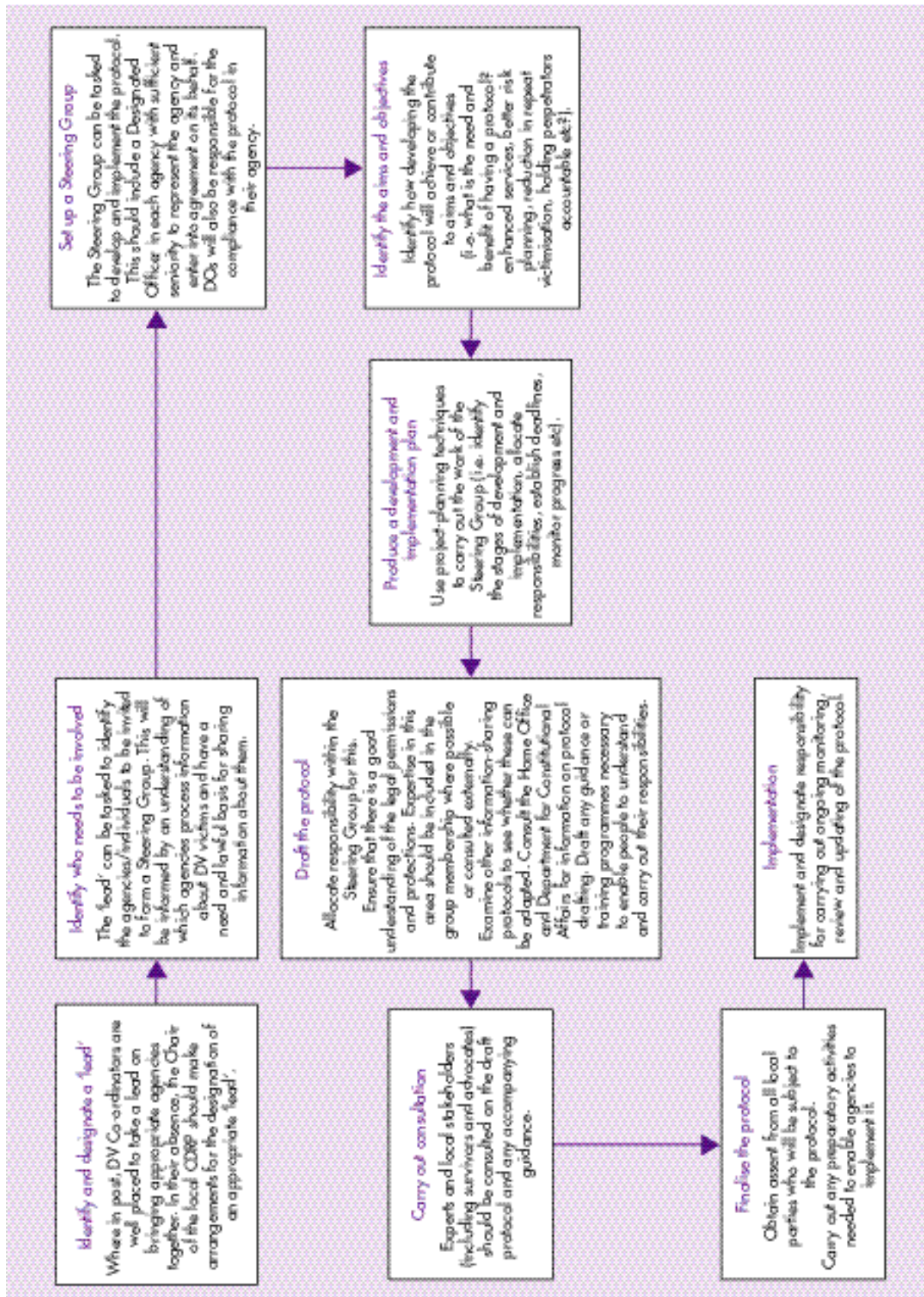
Paragraph 8: The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject.

Paragraph 9: The processing is necessary for ethnic monitoring purposes.

Paragraph 10: The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes. The Data Protection Processing of Personal Data Order 2000 (SI 2000 No 417) specifies a number of circumstances in which sensitive personal data may be processed such as crime prevention, policing and regulatory functions (subject to a substantial public interest test); counselling (subject to a substantial public interest test); insurance, equality monitoring in the area of disability and religious or other beliefs; and research.

Section 1 of the order permits processing of sensitive personal data that is: (a) in the substantial public interest; (b) necessary for the purposes of the prevention or detection of any unlawful act (or failure to act); and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those [crime prevention/detection] purposes.

Appendix 4: Suggested process for drawing up a domestic violence information-sharing protocol



The Research, Development and Statistics Directorate exists to improve policy making, decision taking and practice in support of the Home Office purpose and aims, to provide the public and Parliament with information necessary for informed debate and to publish information for future use.

Home Office Development and Practice Reports are produced by the Research, Development and Statistics Directorate.

For further copies contact:
Communication Development Unit
Room 264,
Home Office,
50 Queen Anne's Gate, London
SW1H 9AT.

Tel: 020 7273 2084
Fax: 020 7222 0211
E-mail: publications.rds@homeoffice.gsi.gov.uk

Visit our website at <http://www.homeoffice.gov.uk/rds>

© Crown copyright 2004
ISSN 1477 3120
ISBN 1 84473 241 X