

Appendix 3. Multi-Agency Information Sharing

1.0	SUMMARY OF THE LEGAL FRAMEWORK	2-10
	Statutory Powers for Sharing Information	2-4
	Data Protection Act 1998	4-8
	Common Law Duty of Confidence	8
	Human Rights Act 1998	8-9
	Caldicott Committee	10
2.0	INFORMATION SHARING ABOUT THE VULNERABLE ADULT	10-11
	Sharing Information with Carers, Parents, Family, Partners etc.	11
3.0	INFORMATION SHARING ABOUT THE ALLEGED ABUSER	11-13
4.0	CHECKLIST TO ESTABLISH THE LEGALITY OF INFORMATION SHARING	14-16

1.0 SUMMARY OF THE LEGAL FRAMEWORK

It is inappropriate for agencies to promise absolute confidentiality. In cases where there are concerns about abuse, including situations when other people may be at risk, information must be shared with other agencies involved in the care and protection of the vulnerable person(s). This appendix sets out the legal framework for the need to share information.

Statutory Powers for Sharing Information

The first step for a public body seeking to collect, use or share data will be to identify a statutory duty or power enabling it to act. This may be from express or implied statutory powers. As far as adults are concerned the express statutory provisions of direct relevance are as follows:

Local Government Act 1972

Section 111(1) - provides that a Local Authority “shall have power to do anything... which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions”.

Local Government Act 2000

Section 2(1) - empowers Local Authorities, amongst other things, to do anything which they consider is likely to promote or improve the social well-being of their area, provided it is not prohibited by other legislation.

Government guidance encourages Councils to regard s.2 as a power of “first resort” and to use it in appropriate situations rather than searching for a specific power elsewhere.

S2 provides a very wide basis for the sharing of information wherever that information is required to enable the Local Authority to fulfil its functions which promote the well-being of people (including a sub-group such as [vulnerable adults]) within its area. The reduction or elimination of risk factors for [vulnerable adults] will promote their well-being.

The Ministry of Justice advises: Section 2 is of particular relevance as it is designed to ensure that service delivery is co-ordinated in ways which minimise duplication and maximise effectiveness. Section 2 would permit many types of data sharing partnership between Local Authorities and others where the proposed data sharing will achieve one of the objects set out in section 2(1) and where there is no statutory prohibition (express or, in very rare cases, implied) restricting the data sharing proposed.

Section 2(5) makes it clear that a Local Authority may do anything for the benefit of a person outside their area if it achieves one of the objects of section 2(1).

Crime and Disorder Act 1998

Section 115 - authorises (but does not require) relevant Authorities (such as Local Authorities, Health and Police) to disclose information where it is “necessary or expedient” for the purposes of any provision of the Act i.e. the prevention and reduction of crime and the identification and apprehension of offenders or suspected offenders.

S.115 overrides the common law duty of confidence and whilst there is no need to obtain consent from the person to whom the information relates prior to its disclosure, certain general principles still apply i.e. information should only be disclosed on a need to know basis and the minimum amount of information necessary to fulfil the statutory duty should be provided.

Implied Statutory Powers

The Ministry of Justice gives the following guidance:

Where there is no express statutory power to share data it may still be possible to imply such a power.

Many activities of statutory bodies will be carried out pursuant to implied statutory powers particularly as it might be difficult to expressly define all the numerous activities that a public body may carry out in connection with its day to day operations. This is particularly in relation to activities such as data collection and sharing which are not of themselves usually express statutory functions. In order to imply a power to share data, one must first of all be satisfied that the body in question has the vires to carry out the basic function, to which the sharing of data is ancillary. Without the power to do the activity there can be no implicit power to share data.

It is clear that government departments that are created by statute do have implied powers to share data where there is no express statutory power to do so. There are a number of authorities that support this in the context of disclosing confidential information to prevent wrongdoing. For example, in *R v Chief Constable of the North Wales Police, ex parte AB* [1998] 3 ALL ER 310 the extent of data sharing power was considered in relation to the disclosure of information about paedophiles to individuals living in an area that put them at risk. Here it was accepted that the police have the power (either implied statutory or common law) to disclose information for the purposes of performing their public duties.

A similar conclusion was reached in the case of *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25 where it was accepted that the police had the power to disclose information to a regulatory body for the purposes of an inquiry as this was in the public interest. Here, there was clearly a strong public interest for making the disclosure in question.

In *Maddox v Devon Council* the Council had disclosed information extracted from its files to a university at which Mrs Maddox had obtained a place to study to become a social worker. She argued the information gave an unfair and misleading impression of her in relation to her parenting skills and her fitness to be a social worker.

The council accepted that there was an obligation of confidentiality in respect of the files, but argued that the disclosure of the information was necessary in the public interest. In particular, the council was concerned about her fitness to be a social worker given that social services had been involved in the upbringing of her son (S) almost since his birth. S had exhibited considerable signs of disturbance during his childhood and she had refused to accept any responsibility for his difficulties. His name was eventually placed on the child protection register on the basis of emotional abuse.

The Court held that the council's disclosure was not a disproportionate reaction to the perceived problem. It was proper for the council to draw the university's attention to its concerns so that the university could make its own decision. It was a matter of public interest that unsuitable persons should not become social workers.

The primary obligation lay on the council to decide whether or not to make the disclosure and there was no requirement for it to obtain a ruling from the court before doing so. In general, as a matter of good practice, before making a disclosure in a case such as the present, a party in the council's position should inform the subject of the disclosure of that intention in enough time to enable that person to seek an injunction from the courts.

Data Protection Act 1998

The Data Protection Act applies to personal data which relates to a living individual who can be identified from those data. It includes:

- (i) information processed, or intended to be processed, wholly or partly by automatic means (that is, information in electronic form usually on computer)

- (ii) information processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is usually paper records in a filing system)
- (iii) information that forms part of an 'accessible record' (that is, certain health records, educational records and certain local authority housing or social services records, regardless of whether the information is processed automatically or is held in a relevant filing system)
- (iv) information held by a public authority (referred to as 'category 'e' data' as it falls within paragraph (e) of section 1(1) of the DPA). This is personal information which is in the possession of the authority, but which has not been entered into the records, This might include, for example, information held by social or care workers on laptops or paper reports which have been received but are not yet filed.

It includes any expression of opinion about the individual and any indication of the intentions of any person in respect of the individual.

It applies to anything at all done to personal data ("processing"), including collection, use, disclosure, destruction and merely holding data. Even disclosing personal data from one part of an organisation to another will amount to processing.

Organisations processing personal data ("controllers") must comply with the data protection principles. The key principles for the purposes of this guidance are that data must be:

- fairly and lawfully processed (1st):- this requires, amongst other things, that there must be a statutory power enabling the processing and that the person from whom the data is obtained must not be deceived or misled as to the purposes for which the data is to be processed. You cannot use information obtained for one purpose for another "incompatible" purpose. It is a particular requirement that the conditions of Schedules 2 and 3 (see below) are met.
- processed only for specified, lawful and compatible purposes (2nd)
- adequate, relevant and not excessive (3rd)
- accurate and where necessary, kept up to date (4th)
- kept for no longer than necessary (5th)
- kept secure (6th)

Personal Data

Sharing of personal data is legitimate (Schedule 2, Data Protection Act 1998) if at least one of the following applies:

- (1) with the data subject's consent, which may be implied
- (2) for compliance with any legal obligation (other than contractual)
- (3) to protect the vital interests of the data subject.
- (4) where processing is necessary: for the administration of justice or the exercise of any powers conferred on any person by or under enactment. This will cover data processing carried out pursuant to express statutory powers or reasonably required or ancillary to the exercise of express or implied statutory powers.
- (5) for the legitimate interests of the data controller unless outweighed by the interests of the data subject.

Sensitive Personal Data

"Sensitive personal data" includes information regarding a person's physical or mental health, sexual life, racial or ethnic origin, political/religious/other opinions and beliefs, trade union membership and commission or alleged commission of offences. The sharing of sensitive personal data is legitimate (Schedule 3, Data Protection Act 1998) if at least one of the following also applies:

- (1) with the explicit consent of the data subject.
- (2) necessary ,
 - (a) in order to protect the vital interests of the data subject or another person, in a case where -
 - (i) consent cannot be given by or on behalf of the data subject, or
 - (ii) it cannot reasonably be expected to obtain the consent of the data subject, or

- (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
- (3) necessary for administration of justice or in the exercise of functions conferred by an enactment.

(N.B. The Information Commissioner has advised that “vital interests” should be equated with life or death situations).

Exemptions

There are a number of important exemptions contained in the DPA that may be relevant in the context of public sector data sharing, although as a matter of good practice public bodies wishing to share data should seek to do so in accordance with the data protection principles where possible, even if an exemption is available.

Certain exemptions apply to “non-disclosure provisions” which are defined in section 27(3) and (4) as including:

- (a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3, and
- (b) the second, third, fourth and fifth data protection principles, (see above), to the extent to which they are inconsistent with the disclosure in question”.

This is an important caveat, as if in any particular case compliance with (for example) the fairness requirement in the first data protection principle is not inconsistent with the disclosure in question, there will be no exemption from that requirement.

Section 29 of the DPA exempts from certain provisions of the Act personal data processed for (i) the prevention or detection of crime; (ii) the apprehension or prosecution of offenders; but only where the application of those provisions would be “likely to prejudice” any of these purposes. This exemption applies to, among other things, the First Data Protection Principle (except to the extent to which it requires a compliance with Schedules 2 and 3) and the non-disclosure provisions. Accordingly, this exemption would cover disclosure of personal information for the specified purposes provided that a Schedule 2 or Schedule 3 condition is also met. Public bodies may benefit from this exemption particularly those for whom the investigation of crime or the prosecution of offenders is their primary purpose.

It should be noted that the “likely to prejudice” test is not a light one and must be satisfied in the circumstances of a particular case; thus the exemption must be applied on a “case by case” basis and could not be used to justify routine data matching or sharing.

Common Law Duty of Confidence

The processing of both personal and sensitive personal data may be shared (without consent), under the Data Protection Act if necessary for a particular statutory function. Certain functions have been identified above.

However, even if you can satisfy the Data Protection Act “necessity” test, it is imperative to consider whether a common law duty of confidence attaches to the data.

Information will be regarded as confidential where it is reasonable to assume in circumstances that the provider of the information expected it to be kept confidential. A duty of confidence is characteristic of several types of relationship such as medical (doctor/patient), legal (solicitor/client) and caring (counsellor/client). However, a duty of confidence does not necessarily arise just because a document is marked “confidential”, although such a marking may be indicative of an expectation of confidentiality.

Information provided by a family to a social worker in the course of that social worker’s functions in giving assistance to that family will be confidential to the family.

Where a clear duty of confidence arises, the information cannot be disclosed to “third parties” without either consent or the requirement of an overriding public interest. It will also be overridden by an express statutory duty such as is found in s.47 of the Children Act or s.115 of the Crime and Disorder Act. There will be a clear public interest in disclosing the data where there is a risk to the life of the vulnerable adult or that they will be seriously injured. In deciding whether or not disclosure of information given in confidence is justified you need to weigh the harm that would result from the breach of confidence against the harm that might result from a failure to disclose. Any disclosure must be proportionate and the minimum necessary to achieve the public interest objective.

Human Rights Act 1998

Public authorities must, of course, act in a way that is compatible with and promotes individuals’ rights under the European Convention of Human Rights and all legislation must be read and interpreted as far as possible in a way which is consistent with those rights. Even if a statutory power to share information has been identified and any common law duty of confidentiality overridden, the disclosure must still comply with the Human Rights Act.

Article 3 - no-one shall be subjected to inhuman or degrading treatment.

Article 8 - guarantees an individual's right to respect to their private and family life. Interference with this right by a public authority can only be justified if:-

- (1) It is in accordance with a statutory or other power authorising disclosure.
- (2) It is necessary for one of the following reasons
 - (a) the prevention of disorder or crime.
 - (b) the protection of health or morals.
 - (c) the protection of the rights and freedom of others.
- (3) The interference (e.g. the disclosure) was proportionate i.e. only to the extent necessary to achieve the particular pressing purpose.

Disclosure of information to safeguard a vulnerable adult will usually be for one or more reasons set out in paragraph (2) above.

In order to satisfy this criterion, it must be shown that the managing and assessing of the risk could not effectively be achieved other than by the sharing of the information in question.

In the House of Lords case of *R v Secretary of State for the Home Department, ex parte Daly* [2001] UKHL 26 Lord Steyn set out a new test to be adopted by the courts in assessing the proportionality principle. In his judgment he emphasised the high level of intensity of review under the proportionality approach in that:

- The reviewing court may need to assess the balance which the decision maker has struck;
- The court may need to direct attention to the relative weight accorded to interests and consideration;
- The proportionality test may require the court to go further than the test of "heightened scrutiny" previously adopted on judicial review. The more substantial the interference with human rights, the more the court would require by way of justification before it was satisfied that the decision was reasonable. However, the court would still only interfere with an administrative decision where it was satisfied the decision was beyond the range of reasonable responses open to a reasonable decision maker.

Caldicott Committee (Report on the Review of Patient Identifiable Information)

The principle findings of this report as summarised in No Secrets are as follows:

- information will only be shared on a “need to know” basis when it is in the best interests of the service user,
- informed consent should be obtained but, if this is not possible and other vulnerable adults are at risk, it may be necessary to override this requirement.

2.0 INFORMATION SHARING ABOUT THE VULNERABLE ADULT

The “No Secrets” document says that the government expects agencies to be sharing information about clients who may be at risk from abuse. There is a general discussion below but, in addition a checklist has been developed to assist in the decision making process.

It is important to identify an abusive situation as early as possible so that the individual can be protected. Withholding information may lead to abuse not being dealt with early enough. Confidentiality must never be confused with secrecy.

It is advised that all agencies use the following guidance regarding the sharing of information with each other;

All clients should be informed at the first visit, or as part of the ongoing assessment, (even when abuse is not suspected) when and why their information will be shared with other service providers or Assessment Teams. This should be explained verbally, and backed up by giving written information (please use leaflet provided within this appendix). Where the client is unhappy with this, the client records/notes should reflect their concerns.

Ideally, the client should be told BEFORE any information is passed on. This may not always be possible. If it is necessary, or the service user does not have the “capacity” to understand the information being given to them, information should be shared between agencies without the consent of the individual.

Information will only be shared on a ‘need to know basis’. Only information relevant to the immediate situation needs to be disclosed and information will be shared **only** for the purpose of providing care or for the protection of vulnerable adults.

All decisions made about withholding or sharing information **must** be recorded, particularly where the consent of the subject of the information has not been obtained.

The sharing of information **must** always be discussed with a line/senior manager and/or Legal Services/Advisor.

Decisions about who needs to know and what needs to be known should be taken on a case by case basis.

There will be circumstances when a duty to protect the wider public will outweigh the responsibility to any one individual. If it is assessed that the service user continues to pose a threat to other service users then this should be included in any information that is passed on to service providers.

While papers and records about the vulnerable adult belong to the agency, the information belongs to the person themselves. The views and wishes of the vulnerable adult will **normally** be respected unless it is thought that they are in a situation which results in their abuse or if it is thought they may be abusing another person(s).

Decisions to share information about the vulnerable adult **must** be made by the agency and not any member of staff acting on their own.

Information given to an individual member of staff, or agency representative, belongs to the agency **not** that member of staff.

Sharing Information with Carers, Parents, Family, Partners etc.

When the vulnerable adult has the “capacity” to make the decision, it should be up to them to decide what information is disclosed to their carers/parents/family/partners. The client records/notes should reflect this. When the adult does not have capacity, consideration should be given to when to share information with carers/parents of vulnerable adults. Clear decisions should be recorded about when to share, what to share and who is the most appropriate person to talk to the carer/parent. Generally some assessment should be made as to whether the sharing of certain information with a particular person or organisation is in the adult’s best interests.

3.0 SHARING INFORMATION ABOUT THE (ALLEGED) ABUSER

Where cases have gone to Court in this area they have often concerned a decision by a Local Authority to disclose information about an individual thought to pose a risk to children, rather than sharing personal data relating to a specific child or vulnerable adult.

The Local Authority must “honestly and reasonably believe” that the sharing of information is necessary to protect a vulnerable adult and must use the test of “pressing social need”. To pass this test the relevant agency must consider the following issues:-

- (1) How strong is their belief in the truth of the particular allegation? The greater the conviction that the allegation is true the more compelling the need for disclosure.
- (2) What is the interest of the third party in receiving the information? The greater the legitimacy of the interest in the third party in having the information the more important the need to disclose.
- (3) What is the degree of risk posed by the individual if disclosure is not made?

Decisions about who needs to know and what needs to be known should be taken on a case by case basis. It is vital there is a balancing exercise undertaken weighing the serious consequences of disclosure against risks to the vulnerable adult. Clearly the issue of proportionality will be vital.

Disclosures to other agencies outside of the Vulnerable Adult Safeguarding Board

There may, exceptionally, be some cases where the risk posed by an individual in the community cannot be managed without the disclosure of some information to a third party outside the statutory agencies. For example, where an employer, voluntary group organiser or church leader has a position of responsibility/control over the individual and other persons who may be at serious risk.

The principles underpinning disclosure to third parties are the same as for information sharing, but inevitably involve greater sensitivities given that disclosure may be to individual members of the public as opposed to central or local government or law enforcement bodies. Because of this, great caution should be exercised before making any such disclosure: it should be seen as an exceptional measure. The following checklist may be of assistance:

- the individual presents **a risk of serious harm** to the vulnerable adult, or to those for whom the recipient of the information has responsibility;
- **there is no other practicable, less intrusive means of protecting the vulnerable adult , and failure to disclose would put them in danger.** Also, only that information which is necessary to prevent the harm may be disclosed, which will rarely be all the information available;

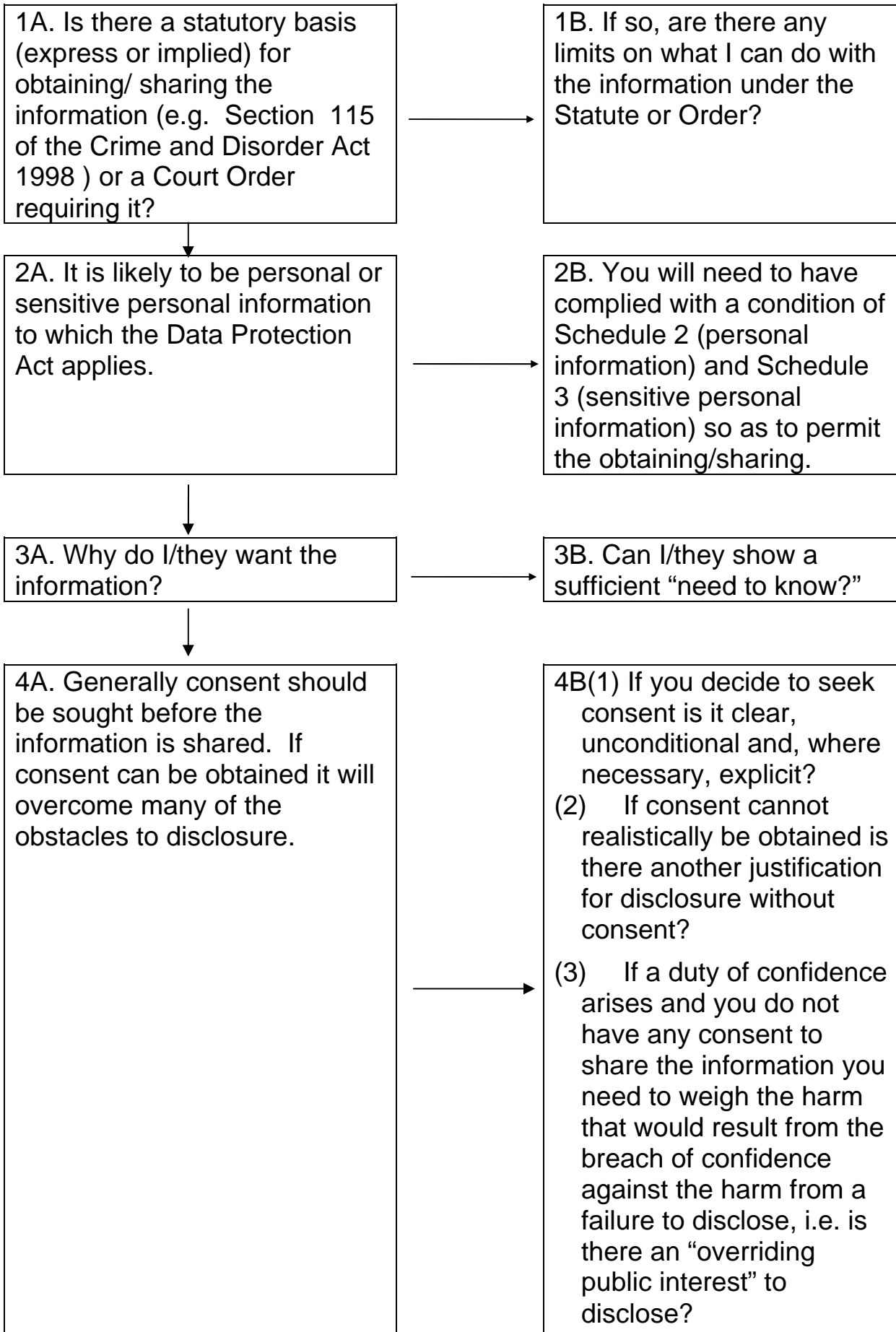
- **the risk to the individual should be considered although it should not outweigh the potential risk to others were disclosure not to be made.** The individual retains his rights (most importantly his Article 2 right to life) and consideration must be given to whether those rights are endangered as a consequence of the disclosure. It is partly in respect of such consideration that widespread disclosure of the identity and whereabouts of an individual is very, very rarely if ever justified;
- **the disclosure is to the right person** and that they understand the confidential and sensitive nature of the information they have received. The right person will be the person who needs to know in order to avoid or prevent the risks;
- **consider consulting the individual** about the proposed disclosure. This should be done in all cases unless to do so would not be safe or appropriate. If it is possible and appropriate to obtain the individual's consent then a number of potential objections to the disclosure are overcome. Equally, the individual may wish to leave the placement rather than have any disclosure made, and if this is appropriate, this would also avoid the need for any disclosure;
- **ensure that whoever has been given the information knows what to do with it.** Again, where this is a specific person, this may be less problematic but in the case of an employer, for example, you may need to provide advice and support; and
- before actually disclosing the information, particularly to an employer or someone in a similar position, **first ask them whether they have any information about the individual.** If they have the information then no disclosure is necessary. If they have some but possibly incorrect information your disclosure can helpfully correct it.

Storing information

Good practice should ensure that all personal information is kept securely and is shared with and available only to those who have a legitimate interest in knowing it.

Essentially, arrangements must be in place which ensure that information is only shared with those with a legitimate interest and cannot by accident or design be accessed by others.

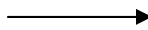
4.0 CHECKLIST TO ESTABLISH THE LEGALITY OF INFORMATION SHARING



5A. You need to be able to demonstrate that you have considered Article 8 of the European Convention of Human Rights, i.e. the right to respect to a private and family life. Your recorded reasons for sharing the information should make reference to this

5B. Is the disclosure

- (1) in accordance with a statutory or other power authorising disclosure?
- (2) necessary for the prevention of crime/disorder or for the protection of
 - (i) health or morals, or
 - (ii) the rights and freedom of others
- (3) proportionate i.e. only to the extent necessary to achieve the particular pressing purpose.



6A. Will there be a further disclosure to a “third party”? Consider all of the questions in this checklist and see



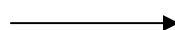
7A. Do you intend to share information about an (alleged) abuser (as opposed to a specific vulnerable adult)? Consider all of the questions in this checklist and see (vi). Do you “honestly and reasonably” believe there is “pressing need” to share information so as to protect vulnerable adults?

Consider the following:

- (1) How strong is your belief in the truth of the particular allegation?

7B.

- (1) The greater the conviction that the allegation is true the more compelling the need for disclosure.



(2) What is the interest of the third party in receiving the information?
(3) What is the degree of risk posed by the individual if disclosure is not made?

(2) The greater the legitimacy of the interest of the third party in having the information the more important the need to disclose.

8A. Consider consulting (rather than seeking consent from) the individual about any proposed disclosure.

8B. This should generally be done unless it would increase the risks of harm. Often it will be appropriate to inform the individual of a proposed disclosure in sufficient time to enable that person to seek an injunction.

9A. Are you satisfied that the practical systems are sufficiently secure and controlled to ensure that the information will only be seen by those who need to know. (see (vii))

9B. Disclosure must be to the correct person i.e. the person who can avoid/prevent the risks. They must know what to do with it and understand its confidential and sensitive nature.

10A. Ensure that only that information which is necessary to prevent harm is disclosed. It will rarely be all the information available.

10B. Consider asking the potential recipient whether they already have any relevant information. If they do disclosure may not be necessary.