EAST AYRSHIRE COUNCIL

SOCIAL WORK COMMITTEE: 3 NOVEMBER 2005

INFORMATION SHARING PROTOCOL

Report by the Executive Director of Educational and Social Services

1. PURPOSE OF THE REPORT

1.1 To seek the approval of Social Work Committee for a Joint Information Sharing Protocol between NHS Ayrshire and Arran, East Ayrshire, North Ayrshire and South Ayrshire Councils.

2. BACKGROUND

2.1 The publication of the report, 'For Scotland's Children – Better Integrated Children's Services' and other significant national enquiry reports has highlighted the need for development of this Information Sharing Protocol to support effective integrated working across a range of children's services.

2.3 The Protocol has also been approved by East Ayrshire Multi-Agency Child Protection Committee which has representation from a range of partner agencies including Local Authority, Health, Police and Scottish Children's Reporters Administration.

2.4 The key agencies involved in this Information Sharing Protocol are the Local Authorities and Health Services.

3. CONTENT OF THE INFORMATION SHARING PROTOCOL

3.1 The protocol is to ensure the exchange of information that is necessary to enable multi-agency and multi-disciplinary work. It also highlights that this exchange of information must be controlled, transparent and compliant with the relevant legal and ethical requirements. Workers must be aware that only relevant personal information should be shared on a 'need to know' basis.

3.2 The protocol clearly states that if a child has or is likely to suffer significant harm then information should be shared with the relevant statutory agencies. In such circumstances consent to share information is not necessary but where safe to do so should be sought.

4. PERSONNEL/LEGAL IMPLICATIONS

4.1 Nil.

5. FINANCIAL IMPLICATIONS

5.1 Nil.

6. COMMUNITY PLANNING IMPLICATIONS

6.1 The introduction of the protocol supports the community planning process in respect of multi-agency working.

7. RECOMMENDATIONS

7.1 Members of the Social Work Committee are invited to:

(i) endorse the introduction of the protocol in children's services; and

(ii) otherwise note the content of this report

John Mulgrew
Executive Director of Educational & Social Services
6 October 2005
Enc (1)

LIST OF BACKGROUND PAPERS

1. For Scotland's Children – Better Integrated Children's Services – Scottish Executive 2001.

For further information on this report please contact: Sally Ann Kelly, Senior Manager Children & Families and Criminal Justice, telephone: 01563 576845

IMPLEMENTATION OFFICER: JACKIE DONNELLY

Information Sharing Protocol

Version Number:
3.0
Prepared By:
Data Protection Officer
Effective From:
Sept 2004
Review Date:
Sept 2005
Ratification Process:
North Ayrshire Council *South Ayrshire Council* *East Ayrshire Council* *NHS Ayrshire & Arran*

It should be noted that although this protocol has been developed to support the Single Shared Assessment of Community Health Needs and the Integrated Assessment Framework for Children in Need, the principals contained within could be applied to other areas of practice. Local operational procedures will require to be written to enable staff within the various agencies to facilitate implementation of the protocol for other purposes.

The group involved in the development of the protocol has identified that a system to record consent is required which will allow agencies to share information whilst at the same time ensure their compliance with current legislation.

The Health Council, as client/patient representatives, was given the opportunity to comment on the protocol.

TABLE OF CONTENTS

1. Introduction

1.1. The aim of public policy is that individuals receive the services that they need and that the organisation of services should not impede or debase the service provided. This clearly requires agencies to work effectively and efficiently together to tailor services to the particular circumstances of each individual. Sharing information about an individual is vital to the provision of co-ordinated and seamless care to that individual service user.

1.2. This protocol is designed to ensure that the exchange of information which is necessary to permit multi-agency and multi-disciplinary service can proceed in a way which conforms with all applicable laws and safeguards the rights of the parties and service users.

1.3. Information sharing, particularly where it involves the sharing of confidential details about individuals, must be controlled, transparent and compliant with relevant legal and ethical requirements. Appropriate security measures need to be in place to safeguard information.

1.4. Personal information falls into two separate categories; personal information and sensitive personal information – see Appendix 1 for the definition of Sensitive Personal Data as determined by the Data Protection Act 1998. The conditions under which the information may be released will depend on which category the information falls into.

1.5. Medical records are sensitive personal information in terms of the Data Protection Act 1998 and may be made available where necessary for medical purposes. Only under exceptional circumstances, for example when required by statute, will complete client/patient records be passed outwith the originating organisation without the patient's consent, if the release of the records cannot be justified on the grounds of medical necessity, even if these are anonymised.

1.6. Where the information to be released is not sensitive personal information, and cannot identify individuals, i.e. where it has been anonymised - it may be shared to support legitimate activity without the consent of the individual, for example, for research, statistical or planning purposes - However, it should be noted that even when personal information has been successfully anonymised, individuals must still be informed of the proposed use(s) of this anonymised information. Staff are encouraged to use anonymised data wherever practicable to safeguard privacy and confidentiality.

1.7. The necessary control, transparency and assurances that appropriate standards of confidentiality and security will be met can best be achieved through the development of information sharing protocols such as this.

.

1.8. Personally identifiable information, held in both manual and electronic format, is collected in order that individuals may receive quality services from the agencies below:

NHS

- NHS Ayrshire & Arran

Local Authorities:

- South Ayrshire Council
- East Ayrshire Council
- North Ayrshire Council

1.9. All bodies will hereafter be referred to as the 'agencies'.

1.10. The agencies acknowledge that under certain circumstances there is a need to disclose personal information/data between each other to ensure that on-going services are not compromised yet ensuring confidentiality is maintained at all times.

1.11. This document outlines the terms and conditions agreed between the agencies under which identifiable Information needs to be shared and the safeguards that must be implemented.

1.12. It should be noted that staff within NHS Ayrshire & Arran must adhere to the principles and recommendations within the Caldicott Review and that patient identifiable information may only be shared on a strict 'need to know' basis. Similarly, in accordance with the requirements of the Common Law Duty of Confidentiality, information originally given in confidence may only be shared with either consent; in the public interest or by law.

2. Objectives

The objectives of this Protocol document are to:

2.1. Set parameters for the sharing of information between agencies which contribute to multi agency intervention plans

2.2. Define how individuals shall be informed of the sharing of their personal information between the agencies.

2.3. Ensure appropriate procedures are in place to support staff in obtaining valid informed consent for the information sharing process.

2.4. Define the purposes for holding personal information within each agency.

2.5. Define how personal information should be held within each agency, who should have access to this information, how long it should be held and the manner in which it should be destroyed.

2.6. Provide a framework to ensure that an individual's confidentiality is maintained at all times.

3. General Principles

The general principles under which this Protocol will operate are as follows:

3.1 In order to ensure individuals receive quality services, it is vital that information be shared and that those staff involved have ready access to the information they need. Individual service users and their carers must have implicit trust that their personal information will be kept secure and confidential and that their privacy is respected at all times.

3.2 All staff have an obligation to safeguard the confidentiality of personal information. This is governed by law (Data Protection Act 1998), the Common Law Duty of Confidentiality, contracts of employment and also by professional codes of conduct. All staff must be aware that any breach of confidentiality could be a matter for disciplinary action or provide grounds for complaints against them on an individual basis.

3.3 It may not be practical nor necessary to seek an individual's specific consent each time personal information needs to be passed on for a particular purpose defined within this protocol (see Section 5 – Defined Purpose). However, individuals always must be fully informed of the uses to which their information may be put. All agencies concerned with the care of individuals or in the use of personal information must satisfy themselves that this requirement is met.

3.4 Where an individual states that they do not want their personal information divulged the individual's wish should be respected unless there are exceptional circumstances (see 3.5 below). Individuals should be informed that withholding information may result in difficulties or delays in the provision of services but no pressure should be put on the individual to agree to the disclosure of their data.

3.5 Exceptional circumstances in which an individual's right may be overridden would include where information is required by statute or court order, where there is serious risk to public health, risk of harm to other individuals or for the prevention, detection or prosecution of serious crime. Where there is the potential for harm to children or where children have already been identified as being at risk through child protection procedures, then the need for consent is overridden and information should be shared with appropriate agencies.

Each employing Agency has a statutory duty to manage the risk to safety of their own staff and to exercise a duty of care towards persons not in their own employment, therefore it is essential to consider the implications of non-compliance with the Health & Safety at Work Act 1974 in conjunction with requirements of the Data Protection Act 1998 and the Common Law Duty of Confidentiality.

3.6 Even where information has been aggregated/anonymised, it can still only be used for justified purposes and although consent may not be required, the individual to whom the information relates must be informed. Care must be taken to remove all possible identifiers from this type of information.

3.7 Access to personal information must be controlled on a strict need to know basis and therefore only minimum identifiable information to satisfy the purposes required should be made available.

4. Agreed Parameters

4.1 There will be one nominated Senior Professional Officer within each agency as follows - Director of Public Health; Medical Directors; Heads of Social Work who will be responsible for agreeing the Protocol and any subsequent amendments. All proposed amendments must be made in writing and signed by the agreed nominated Senior Professional Officer(s). No amendments will otherwise be accepted.

4.2 Personal information will be transferred between the agencies as agreed within the terms of this protocol. Each agency must maintain up-to-date registers of personnel and access rights for personal information. Staff within agencies will be assumed to have access rights in accordance with Caldicott principles and recommendations (see 1.12).

4.3 Specific consent will be required for transmission of personal information for purposes other than those defined in the Protocol. Requests for any access other than those identified must be submitted to the nominated Senior Professional Officers. Proof of such consent will be required prior to any information being transferred.

4.4 Where a person does not have the capacity to make an informed decision but a third party has authority to act as their guardian and take decisions on their behalf, then the information sharing protocol and all that is included in it must be explained to that third party in the same manner that it would initially have been explained to the individual.

4.5 In the absence of a legal or welfare guardian – see Part 6 – Adults with Incapacity (Scotland) Act 2000 - the decision should be made on the individual's behalf by those responsible for providing care, taking into account all known views, with the individual's best interests being paramount. The reasons for the final decision must be clearly documented and signed by the appropriate nominated Senior Professional Officer(s).

5. Defined Purposes

5.1 The following are purposes agreed as justifiable for the transfer of personal information between agencies, as defined within the remit of this Protocol. It should be noted however that the list is not exhaustive. All staff are reminded that only **relevant** personal information should be shared on a 'need to know' basis and that they have a responsibility to make themselves aware of the circumstances of each individual situation:

- Delivery of integrated services
- Assuring and improving the quality of services
- Monitoring, reporting and protecting public health
- Managing and planning future services*
- Contracting for services*
- Auditing accounts and performance
- Statutory obligation
- Risk management
- Court orders
- Research/trials*
- Statistical analysis*
- Investigation of complaints or potential legal claims*
- Medical reports/insurance requests*
- Child Protection

if **identifiable personal information is shared for the purposes marked with an asterisk above, the consent of the individual must be obtained. This consent may be implied or explicit dependent upon local operational procedures. Where consent is not obtained, the data must be stripped of all identifiers (see Section 1.6).*

6. Obtaining Consent

6.1 To support staff, each agency will put in place procedures that give clear guidance on seeking consent. A flowchart for determining disclosure is at Appendix 2.

6.2 Any member of staff, who may have to seek the consent of a person to share information about them must understand and be able to explain the purpose and implications of sharing information, what this may entail, and the safeguards of confidentiality that apply.

6.3 Consent will be sought at the earliest opportunity and **at the very least** prior to information being shared with any other agency. It is the responsibility of agencies to ensure that consent is given on an informed basis and clear information should be available for individuals and staff who use and deliver services

6.4 Within individual agencies, implied consent may be acceptable in circumstances where an individual will be a participant in the process and would expect identifying information to be recorded and seen by those involved in providing the care within that agency. When the information requires to be shared between agencies explicit consent is required.

6.5 In cases where implied consent is accepted, each agency must be able to demonstrate that the requirement to inform has been fully implemented and that refusals or withdrawals of consent are recorded and dealt with effectively.

6.6 Personally identifiable information must not be shared for education, training or research purposes without explicit consent, for example identifiable records used as training aids.

6.7 Each agency must have an up to date storage retention & destruction policy for personal information.

6.8 Sections 3.5; 4.4 & 4.5 outline exceptional circumstances when obtaining consent.

7. Recording Consent

7.1 Agencies must have a means by which an individual or their guardian can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure. These limitations should only be over-ridden if there are statutory grounds for doing so.

7.2 Each agency must ensure that all systems recording consent, whether manual or electronic, must be able to effectively deal with consent being withdrawn at a later date.

7.3 Consent must be reviewed at least annually or whenever a change in the situation dictates.

8. Checking for Consent

8.1 When sharing personal information between agencies, consent must be sought. It is the responsibility of all staff to ensure that they are satisfied that consent has been obtained and how long this consent is valid.

8.2 It is recognised that in particular investigations (e.g. where there are vulnerable adult and/or child protection concerns), the significance of information is not often apparent at the early stages and agencies may put in place procedures that enable them to share all information they hold about the person. In this case, individual protocols will clearly state that such an agreement has been made and will set out the specific arrangements put in place to limit the access to such information to those with a need to know.

9. Disclosing Information without Consent

9.1 Passing information without consent places both individual staff members and agencies at risk of prosecution. If there is no lawful basis for disclosing information without consent, there is also the risk of a compensation order under the Data Protection Act, or damages for breach of confidence/breach of human rights.

9.2 The Health & Safety at Work Act 1974 states that employers have a responsibility to ensure as far as reasonably practicable that persons are not exposed to risks to their health and safety – see para 3.5.

9.3 The disclosure of personal information without consent must be justifiable on statutory grounds and meet one of the conditions of Schedule 2 of the Data Protection Act 1998 (Appendix 4). In addition, if the personal information falls under the definition of 'sensitive personal data' under the Act, a condition of Schedule 3 (Appendix 5) must also be satisfied

9.4 As well as 9.3 above, staff must abide by the requirements of the Common Law Duty of Confidentiality – see para 1.12.

9.5 In some circumstances, the law requires agencies to share information, irrespective of the views of an individual. Best practice would be for the individual to be told about the sharing. An example of this legal requirement may be notification of a notifiable disease, child protection or adoption/fostering issues. In cases such as these the consent of the Senior Nominated Officer is not required.

9.6 Occasionally the sharing of information can be justified as being in the interest of the public as opposed to a specific individual. An example might be the disclosure of information to the police to help in the prevention or detection of a serious crime. Both the Data Protection Act and professional standards specifically allow for information to be shared in this way.

9.7 If data are anonymised the need is to inform but consent is not required. Therefore anonymisation should always be the first consideration when using personal information.

9.8 Individual agencies will have in place local operational procedures which will specify the circumstances under which their staff may disclose information without consent taking into account current legislation and relevant local/national guidance. See para 9.5.

9.9 Each agency will have an on-call executive officer who has the authority and knowledge to take responsibility for decisions taken to share information without consent. This authority will be available outwith normal working hours to enable emergency situations to be dealt with.

10. Access and Security

10.1 Confirmation that all the following standards are in place is required otherwise the agencies may restrict the issue of identifiable information to protect individuals from misuse of information.

10.2 Identifiable information supplied by the agencies must be restricted to staff on a need-to-know basis in order to perform their duties in connection with one or

more of the purposes listed at Section 5 of this protocol. Personal details should be available only to those involved in delivering services to the individual.

10.3 Formal Policies and Procedures must be in place covering the physical security of buildings, security awareness training of staff and security management of systems, both manual and electronic, where identifiable information may be held. The aforementioned agencies reserve the right for external audit of such Policies and Procedures as may be deemed appropriate. Adoption of BS7799 (British Standard in Information Security) will be considered best practice.

10.4 Each agency must take all reasonable care and safeguards to protect both the physical security of information technology and data contained within it.

10.5 All information systems containing identifiable information must be effectively password protected and users must not divulge their password nor leave systems active while absent.

10.6 Each agency must have local operational procedures in place for the secure transfer of personal information.

11. Responsibility for Management of Protocol

11.1 The nominated Senior Professional Officers are ultimately responsible for ensuring the terms of this protocol are adhered to by those staff/agencies to which confidential information is supplied.

11.2 Any breaches of the Protocol must be brought to the immediate attention of the nominated Senior Professional Officer(s)

12. Other Relevant Documentation

12.1 This Protocol has been drawn up taking into account current legislation and guidance documents.

APPENDIX 1

DEFINITION OF 'SENSITIVE PERSONAL DATA' AS DETERMINED BY THE DATA PROTECTION ACT 1998

a) the racial or ethnic origin of the data subject

b) his political opinions

c) his religious beliefs or other beliefs of a similar nature

d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)

e) his physical or mental health or condition

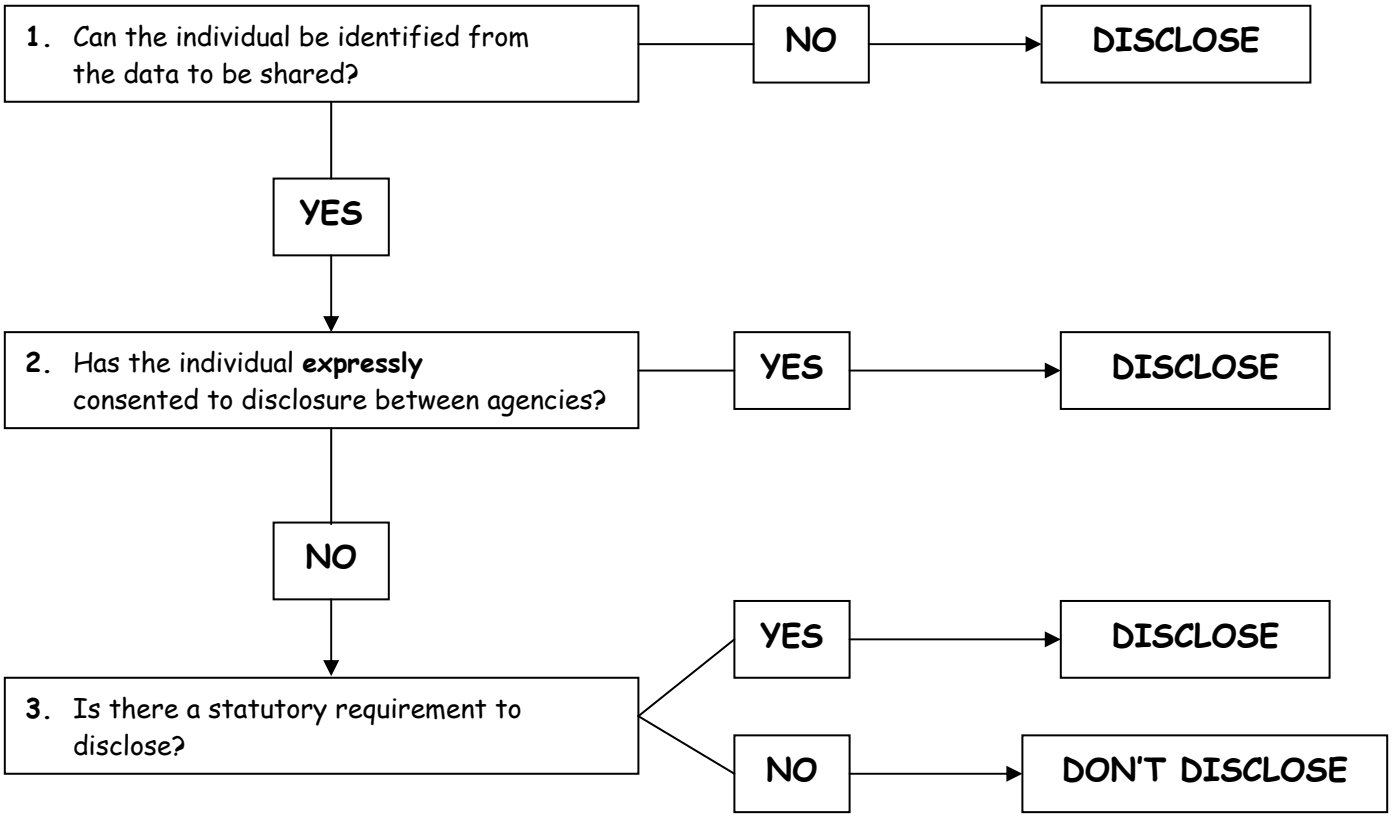
f) his sexual life

g) the commission or alleged commission by him of any offence, or

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

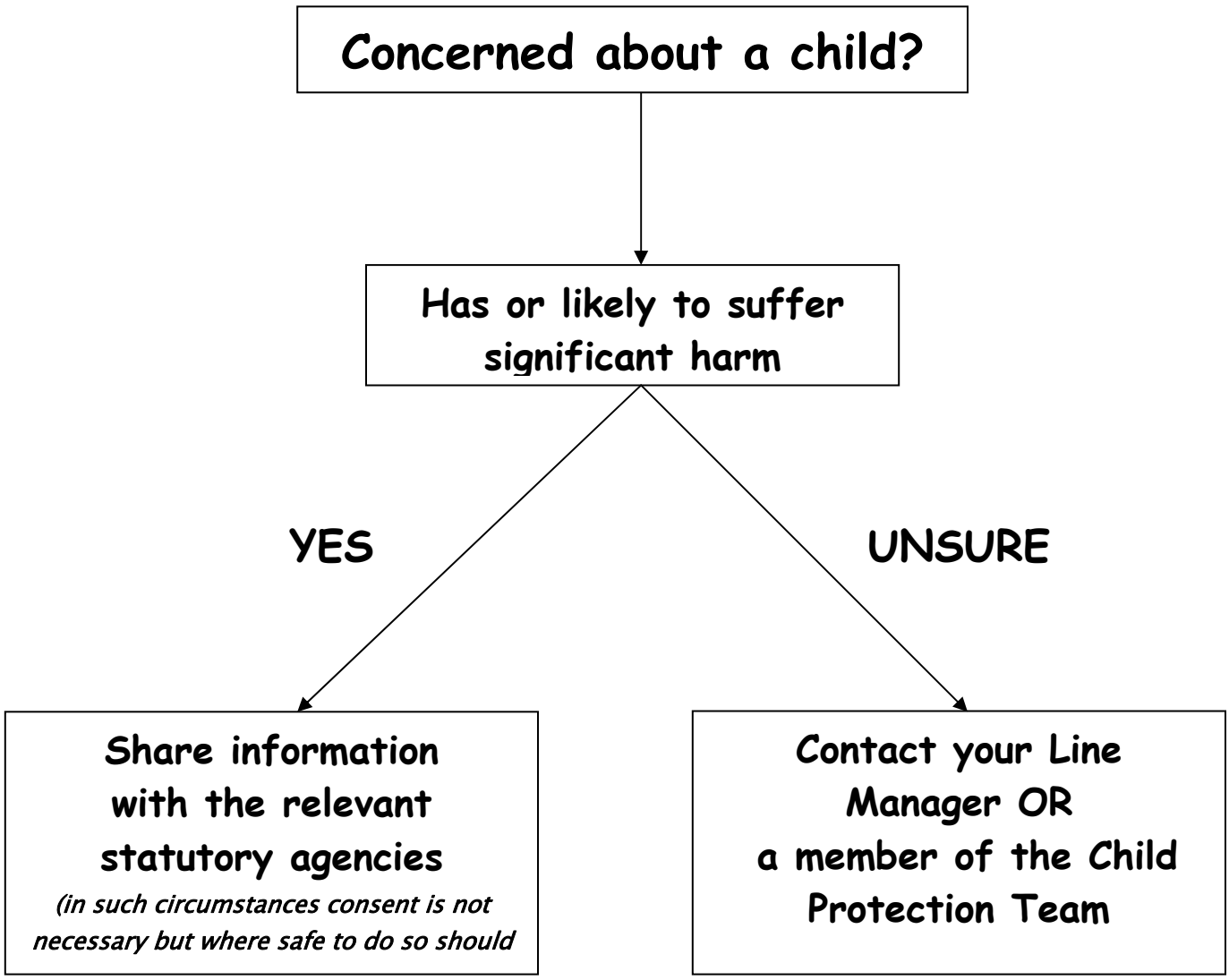
APPENDIX 2

DETERMINING DISCLOSURE



APPENDIX 3

CHILD PROTECTION PROTOCOL MANUAL
SHARING INFORMATION FLOWCHART



APPENDIX 4

DATA PROTECTION ACT 1998 SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

---

1. The data subject has given his consent to the processing.

2. The processing is necessary-
   (a) for the performance of a 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.

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.

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

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 a government department, or
   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

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.
   (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.

APPENDIX 5

DATA PROTECTION ACT 1998 **SCHEDULE 3**
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

---

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
   (2) The Secretary of State may by order-
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is 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) the data controller 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.

4. The processing-
   (a) is carried out in the course of its legitimate activities by any body or association which-
      (i) is not established or conducted for profit, and
      (ii) exists for political, philosophical, religious or trade-union purposes,
   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   (c) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing-
   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   (b) is necessary for the purpose of obtaining legal advice, or
   (d) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

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

   (2) The Secretary of State may by order-
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-
   (a) a health professional, or
   (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

   (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. The processing-
   (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
   (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
   (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

   (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph