Record Keeping, Confidentiality and Sharing Information

8

RECORD KEEPING

8.1 Good record keeping is an important part of a professional's task. Records should use clear, straightforward language, be concise, and accurate. They should clearly differentiate between facts, opinion, judgements and hypothesis.

8.2 Well-kept records are essential to good child protection practice. Safeguarding children requires information to be brought together from a number of sources, and careful professional judgements to be made on the basis of this information. Records must be clear, accessible, and comprehensive. The subject of a record does have the right in law to request access to them at any stage. Judgements made, actions and decisions taken should be carefully recorded. Where decisions have been taken jointly across agencies, or endorsed by a manager, this should be made clear on the case records.

8.3 Relevant information will normally be collated in one place by social services. Records should clearly provide the chronology of the case and should demonstrate how the process has been managed by the professional and indicate how actions taken and decisions made have been endorsed by line managers and senior managers. Specifically, the reader should be able to track the plan for the case through:

- the information about the child and family and actions taken from referral through interventions to outcome and closure of the case;
- identified and potential risks of harm, the source of harm and those at risk;
- the intended outcome for the child, the interventions which have taken place, by whom and the reasons for intervention;
- the evidence that change has taken place; and
- an analysis of the progress that is being made.

8.4 Each agency should ensure that when a child moves outside its area the child's records are transferred promptly to the relevant agency in the new locality. Cases where enquiries do not substantiate the original concerns should be retained in accordance with the agency's record retention policy. This policy should ensure that records are stored safely and can be retrieved promptly and efficiently (see paragraph 5.88).

CONFIDENTIALITY AND INFORMATION SHARING

8.5 Research and experience have shown repeatedly that safeguarding children requires professionals and others to share information about:

- a child's health, development and exposure to possible harm;
- a parent who may need help, or may not be able, to care for a child adequately and safely; and

- those who may pose a risk of harm to a child.

Often, it is only when information from a number of sources has been shared that it becomes clear that a child is at risk.

LEGAL FRAMEWORK

8.6 Personal information about children and families held by professionals is subject to a duty of confidence, and should normally not be disclosed without the consent of the subject. **However, the law permits the disclosure of confidential information necessary to safeguard a child.**

8.7 Professionals can only work together effectively to safeguard children, if there is an exchange of relevant information between them. This has been recognised in principle by the courts. Any disclosure of personal information to others must always, however, have regard to both common and statute law.

8.8 Normally, personal information should only be disclosed to third parties (including other agencies) with the consent of the subject of that information. Wherever possible, consent should be obtained before sharing personal information. In some circumstances, consent may not be obtained, but the safety of the child dictates that the information should be shared. Further guidance is available in the DHSS&PS publication, *The Protection and Use of Patient and Client Information (1999)*

MEDICAL GUIDANCE

8.9 The General Medical Council (GMC) has produced guidance entitled *Confidentiality (1995).* **It emphasises the importance of obtaining a patient's consent to the disclosure of personal information, but makes clear that information may be released to third parties, if necessary without consent, in certain circumstances.** Medical practitioners are advised that:

"If you believe a patient to be victim of neglect or physical or sexual abuse, and unable to give or withhold consent to disclosure, you should usually give this information to an appropriate responsible person or statutory authority, in order to prevent further harm to the patient. In these or similar circumstances, you may release information without the patient's consent, but only if you consider that the patient is unable to give consent, and that disclosure is in the patient's best medical interests".

"Disclosures may be necessary in the public interest where a failure to disclose information may expose the patient, or others, to risk of death or serious harm. In such circumstances you should disclose the information promptly to an appropriate person or authority".

8.10 The GMC has confirmed that its guidance on the disclosure of information which may assist in the prevention or detection of abuse, applies both to information about third parties, for example, adults who may pose a risk of harm to a child, and about children who may be the subject of abuse.

8

NURSING GUIDANCE

8.11 The Nursing and Midwifery Council (formerly UKCC) produced *Code of Professional Conduct (2002),* which contains the following advice at paragraph 5.3:

"If you are required to disclose information outside the team that will have personal consequences for patients or clients, you must obtain their consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

- they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm);
- they are required by law or by order of a court;
- where there is an issue of child protection, you must act at all times in accordance with national and local policies."

SOCIAL WORK GUIDANCE

8.12 *A Code of Ethics for Social Work* adopted by the British Association of Social Workers (BASW) in 2002 states as a principle of practice:

"They (social workers) will respect service users' rights to a relationship of trust, to privacy, reliability and confidentiality and to the responsible use of information obtained from or about them; Observe the principle that information given for one purpose may not be used for a different purpose without the permission of the informant; Consult service users about their preferences in respect of the use of information relating to them; Divulge confidential information only with the consent of the service user or informant, except where there is clear evidence of serious risk to the service user, worker, other persons or the community, or in other circumstances judged exceptional on the basis of professional consideration and consultation, limiting any such breach of confidence to the needs of the situation at the time; Offer counselling as appropriate throughout the process of a service user's access to records; Ensure, so far as it is in their power, that records, whether manual or electronic, are stored securely, are protected from unauthorised access, and are not transferred, manually or electronically, to locations where access may not be satisfactorily controlled; Record information impartially and accurately, recording only relevant matters and specifying the source of information. The sharing of records across agencies and professions, and within a multi-purpose agency, is subject to ethical requirements in respect of privacy and confidentiality. Service users have a right of access to all information recorded about them, subject only to the preservation of other persons' rights to privacy and confidentiality.

DISCLOSURE OF INFORMATION ABOUT SEX OFFENDERS

8.13 The NIO has produced guidance[6] on the exchange of information about all those who have been convicted of, cautioned for, or otherwise dealt with by the courts for a sexual offence; and those who are considered by the relevant

6 *'Guidance on the Processes for the Assessment and Management of Risk of Sex Offenders and Offenders against Children.' (NIO 2001)*

agencies to present a risk to children and others. The guidance also deals with issues about people who have not been convicted or cautioned for offences, but who are suspected of involvement in criminal sexual activity.

8.14 The guidance emphasises that the disclosure of information must take place within an established system and procedure between agencies, and must be integrated into a risk assessment and management system. The police and other relevant agencies should judge each case on its merits, taking account of the degree of risk. The guidance places on the police the responsibility to co-ordinate and lead the risk assessment and management process. It advises that agencies should work within carefully worked out information sharing protocols, and refers to good practice material in existence. It also advocates the establishment of multi-agency risk panels whose purpose is to share information about offenders and to devise strategies to manage their risk. When the alleged or convicted abuser is a child, the information sharing should be managed within the child protection context.

RECORD RETENTION AND DESTRUCTION

8.15 It is the responsibility of staff from individual agencies to maintain their own records of work with child protection cases. Records include those pertaining to the Child Protection Register, child protection case conferences, child abuse investigations, investigations into alleged abuse by professionals. The confidentiality and security of records must be a primary consideration at all times and there must be arrangements in place to facilitate client access. **ACPC procedures must clearly state what happens with any records associated with any part of the child protection process.** Each agency must have a record retention/destruction policy in place which clearly indicates:

- which records will be retained;
- how long records will be held;
- the purpose and format of retained records;
- how records will be retained, with particular emphasis on security;
- how records will be accessed, who has the responsibility for controlling access and levels of access;
- the arrangements for the destruction of records.

8.16 The principles of the Data Protection Act (1998) should be adhered to at all times. A brief outline of the principles is given below. When ACPCs, Trusts and individuals are making decisions about the retention of child protection information, it is worth bearing in mind that the 1998 Act distinguishes between ordinary personal data such as name, address and telephone number and sensitive personal data and that the processing of such data is subject to much stricter conditions.

THE DATA PROTECTION PRINCIPLES

8.17 The eight principles of the Data Protection Act (1998) are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   - at least one of the conditions in Schedule 2 of the 1998 Act is met; and
   - in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the 1998 Act is also met.

8

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the EEA (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.