

# ContactPoint Guidance

**Version 1.0**

**Published 21 July 2008**

## TABLE OF CONTENTS

<b>Topic</b>	<b>Page</b>
<b>INTRODUCTION .....</b>	<b>3</b>
<b>ACCESSING CONTACTPOINT .....</b>	<b>7</b>
<b>USING CONTACTPOINT .....</b>	<b>17</b>
<b>CONTACTPOINT ADMINISTRATION .....</b>	<b>26</b>
<b>Annex A - FLOWCHARTS.....</b>	<b>40</b>
<b>Annex B - LEGISLATION .....</b>	<b>46</b>
<b>Annex C - GLOSSARY AND REFERENCE .....</b>	<b>50</b>

## **1.0 INTRODUCTION**

### **1.01 Purpose of this guidance**

This guidance is issued under section 12(12) of the Children Act 2004 (see B.01), and sets out the key statutory requirements of section 12 and the Children Act 2004 Information Database (England) Regulations 2007 (the Regulations). It also contains non-statutory guidance.

**1.02** The statutory guidance applies to local authorities (LAs -see C15). It also applies to national partners (NPs - see C.19), in relation to their responsibilities for managing users. Those subject to statutory guidance should follow this guidance and, if they decide to depart from it, must have clear and justifiable reasons for doing so.

**1.03** This document also contains non-statutory guidance and is therefore relevant to everyone who will have access to ContactPoint (see 1.15, C.39), whether as a user, administrator or manager. This will help to ensure the appropriate use and operation of ContactPoint in compliance with the Regulations.

This guidance is to be read in conjunction with the Best Practice Processes (BPP - see C.02), and ContactPoint training materials.

**1.04** This guidance is not Information Sharing guidance. Comprehensive guidance on when and how information can be shared is available from the cross-Government '*Information Sharing: Practitioner's Guide*', and related materials (see C.44). These materials are intended to support good practice by offering clarity on when and how information can be shared legally and professionally.

### **1.05 ContactPoint Regulations**

The Regulations (see B.02), place particular duties on local authorities relating to:

- the information to be held on ContactPoint;
- those required or permitted to supply information;
- what information can be disclosed from ContactPoint;
- how long information can be held on ContactPoint;
- ensuring the accuracy of the information;
- how to "participate" in the operation of ContactPoint.

**1.06** The Regulations also place duties on local authorities and national partners relating to:

- who can be given access to ContactPoint (see C.39); and
- the conditions on which access is granted (see 2.28).

### **1.07 Other legislation**

All ContactPoint users must comply with all relevant legislation. This includes the Computer Misuse Act 1990 (CMA - see B.09) and the Data Protection Act 1998 (DPA - see B.10).

### **1.08 Purpose and scope of ContactPoint**

ContactPoint is the quick way to find out who else is working with the same child or young person, making it easier to deliver more coordinated support. ContactPoint will help improve services to children with a strong emphasis on early intervention and prevention, and is a key part of the Every Child Matters programme to improve outcomes for children. ContactPoint comprises a centrally maintained national system with a record for each child.

### **1.09 Appropriate use**

ContactPoint is established under section 12 of the Children Act 2004. Its purpose is to support practitioners, local authorities and other organisations in fulfilling their duties under section 10 (duty to cooperate to improve well-being), and section 11 (safeguarding and promoting welfare of children) of the Children Act 2004, and section 175 of the Education Act 2002 (duty to safeguard and promote the welfare of children). It also supports LA duties established by section 436A of the Education Act 1996 to identify children not receiving education (see B.06).

### **1.10 Child records**

A child record contains information (see C.36), on ContactPoint that relates either to a child (up to their 18<sup>th</sup> birthday) or to a participating young person (see C.21). A participating young person is a person: a) who has consented to information that is not archived information being contained in a child record, and has not withdrawn that consent and b) in relation to whom arrangements under section 10 of the Children Act 2004 may be made. Such arrangements may be made in relation to:

- a) persons aged 18 and 19;
- b) persons over the age of 19 receiving services under the Children Act 1989 (for those leaving care), or;
- c) persons between 19 and 25 with learning difficulties who are receiving services under section 13 of the Learning and Skills Act 2000 (see C.14).

Child records are created in two main ways:

- automatically - using basic demographic data about children from a number of national and local data sources;
- manually - by authorised users with appropriate 'rights' (see BPP1 - Manage Data and BPP4 – Practitioners and Mediators)

### **1.11 ContactPoint can only hold data for children/young people who:**

- are ordinarily resident in England; or
- leave England with the intention to return within three years (e.g. children accompanying parents in the armed forces posted overseas).

Where a child in receipt of a service from an organisation listed in Regulations has supplied an address in England to the organisation, this demonstrates ordinary residence (see C.20) for ContactPoint purposes.

**1.12** Each LA in England is responsible for child records of children and young people who are understood to be ordinarily resident in the LA's area. For looked after children, the council with social services responsibility will be responsible for the child record. ContactPoint will automatically allocate records to a LA based on available data, or by agreement with the LA which previously had responsibility for the child record.

**1.13 How to read this guidance**

This guidance is structured around principles and themes. For each section there is guidance applicable to all readers and guidance targeted at specific user groups in colour-coded, labelled boxes. This is intended to help you quickly identify the guidance relevant to your role. There are also flowcharts, a summary of relevant legislation, a glossary of terms used and signpost to further sources of information.

**1.14 User groups**

The user groups below have been defined for simplicity of reading. Some roles will cover more than one of the user groups defined in this guidance. Therefore users should read all sections relevant to their role.

<b>1.15</b>	<b>User Groups</b>	<b>Roles</b>	<b>Description</b>
	<b>CONTACTPOINT USER</b>	Manager/ supervisor	Team leaders/practice managers of staff who use ContactPoint in the ordinary course of their work and who are also authorised users.
		Practitioner or equivalent	Authorised users who access ContactPoint in order to support their work with children.
		Administrative / support staff or equivalent	Other staff authorised to use ContactPoint to support managers and practitioners in their functions (e.g. school administrator).
	<b>LOCAL PARTNER STAFF</b>	Data Administrator	Responsible for managing data, data quality and supplying data to ContactPoint - not necessarily ContactPoint users.
		User Account Administrator	Responsible for day-to-day administration of agencies' ContactPoint users.
		Staff/Line Manager	Not necessarily ContactPoint users but responsible for those who are.
	<b>LA and NATIONAL PARTNER CONTACTPOINT MANAGEMENT TEAM</b>	ContactPoint Manager	Responsible for the overall operation of ContactPoint in their area (LA only).
		Data Manager	Responsible for maintaining data quality of records for which the LA is responsible (allocated to them).

	User Account Manager	Responsible for establishing and administering ContactPoint user accounts – in an LA or national partner.
--	----------------------	---

## 2.00 ACCESSING CONTACTPOINT

### 2.01 Accuracy

Data held on ContactPoint must be of a sufficiently high quality (see C.09) to be useful. ContactPoint will only be as accurate as the data provided to it by national and local sources and by users.

Everyone who records data must be made aware of the importance of keeping data accurate and up to date in their own case management or (health) patient record systems<sup>1</sup>, and of the consequences, particularly for ContactPoint, of poor quality data.

- 2.02** Everyone who manages personal data, including data managers of systems that provide data to ContactPoint, is bound by the 4th Principle of the DPA, and must take reasonable steps to ensure that the information they provide is accurate and up to date.

This requirement is made explicit in the ContactPoint Regulations, which places duties on LAs and others who provide data to ContactPoint to ensure information provided is accurate and to maintain the accuracy of that information.

- 2.03** **Users** - You play a key role in ensuring that ContactPoint is accurate. You must take all reasonable steps to keep your own CMS records accurate and up to date.

Discrepancies may occur between the records on your own CMS and on ContactPoint. Where you identify, or are notified of, a discrepancy between systems you must take appropriate action to verify and correct the information.

- 2.04** **Data Administrators** of organisations that provide data to ContactPoint are bound by the 4th Principle of the DPA, to ensure that the information you provide is accurate and up to date.

Where errors and discrepancies occur and are known, you must follow your organisation's procedures for rectifying them. Such amendments should be sent to ContactPoint as soon as possible.

- 2.05** **LA ContactPoint Management Teams** - you have, under the DPA and Regulation 5 of the ContactPoint Regulations, a legal duty to ensure the records for which you/your LA is responsible are complete and accurate, and must take reasonable steps to correct the inaccuracy or to complete the record. This may include notifying source systems of any discrepancy.

### 2.06 Security

---

<sup>1</sup> These systems are referred to as case management systems (CMSs) throughout this document.

Security of ContactPoint and the information held on it is of critical importance. Everyone who uses ContactPoint is responsible for maintaining the security and integrity of information on ContactPoint, and must take all practicable steps to ensure that their actions do not compromise security in any way.

**2.07** All users have a responsibility to report security breaches to a nominated person within their organisation, and must be aware of the type of incidents that may be considered a security breach. Security and the importance of good security practice will be covered in ContactPoint training and related materials.

**2.08** Examples of security breaches include, but are not limited to:

- deliberate attempts at hacking;
- sharing of tokens or logins;
- disclosure of passwords;
- leaving a computer logged in but unattended, and any third-party access to an unattended computer;
- public visibility of screens, public invited to view screen;
- misuse of data;
- accessing data that the user has no reasonable need to see;
- unauthorised sharing of data with others;
- user not having received training;
- false claims made at ContactPoint application;
- coercion of users to access and release data (threats, violence, blackmail, bribery)

**2.09** A number of key principles should be observed, as a minimum, by everyone with access to ContactPoint. These are:

- always act in accordance with the DPA and CMA;
- adhere to the ContactPoint security requirements;
- follow any local organisation policy/guidance on IT security;
- comply with relevant security standards (see C.25, C.47);
- never share user accounts, passwords or security tokens with others;
- do not write down your password;
- take care when entering your password to ensure your keyboard is not overlooked;
- keep your security token with you or securely locked up;
- never leave ContactPoint logged in when you leave your desk;
- ensure any reports or information you print from ContactPoint are stored securely and destroyed when no longer required;
- do not let others read ContactPoint information from your computer screen, particularly if working where others could see your computer screen;
- report security breaches to your local security manager;
- keep the information you enter/supply accurate and up to date.

**2.10** Evidence, which may take the form of a declaration that appropriate policies and procedures exist and are followed by all ContactPoint users,

should be made available to the LA ContactPoint Management Team when required.

**2.11** LAs, national partners and local partner organisations should provide guidelines and policies on the secure use of ContactPoint, and ensure that computer workstations are properly configured so as to minimise the likelihood of compromising information held through spyware, viruses and unintended visual access. These requirements are fully set out in the accreditation document and the Detailed Integration Specification (see 4.10, C.01).

**2.12** **Staff Managers** - you are expected to ensure that the workspace in which you and your staff access ContactPoint does not compromise security (see C.47).

You must ensure that all users you manage are aware of the importance of security, understand good security practice and act in a way that will not compromise ContactPoint. It is good practice to ask staff to sign a form containing key security advice to confirm they have read it.

If you suspect a staff member is breaching security, you must take immediate action and alert your organisation's security manager or the LA ContactPoint Management Team, who can advise or may take further action. Where a more serious or intentional breach has occurred, you must suspend the user account immediately and investigate, cooperating fully with your LA.

**2.13** **LA User Account Managers** - you should work with local and national partners to support their responsibilities for managing the security of their systems and users. You must review audit trails for users whose accounts you manage.

**2.14 Passwords**

Failure to keep your password and security token secure may result in suspension or closure of your ContactPoint account. You may also be subject to your organisation's disciplinary procedures. Passwords should be changed on a regular basis.

If you think your password may be known to others, you must change it immediately. If you have lost your security token, you must inform your user account administrator immediately to enable them to take appropriate action.

**2.15** **Users** - you should change your password on a regular basis and prevent others from gaining access to or making use of your account. You must not share your password or security token with others. The only exception is in circumstances where mediated access is required, where you may be asked to partially disclose fragments of your password in order to authenticate your mediated access to ContactPoint (see 2.37, A.3, C.17). Any access to ContactPoint using your password and security token will

register in the audit trail as activity carried out by/for you.

**2.16 User Account Administrators** - where a user reports the loss of their security token or the possibility that their password may be known by others, you must suspend the user account immediately to prevent any unauthorised access (see BPP2 - Manage Users). You can only reactivate a user account after the user has been provided with a new, secure password and/or token. These must be provided via a secure method to a verified person.

**2.17 LA and NP User Account Managers** - you are responsible for managing user accounts and the security arrangements related to them. User accounts and security tokens must only be enabled to authorised users who meet the ContactPoint conditions of access (see 2.28, 2.36).

**2.18 Misuse**

Misuse of ContactPoint is a serious breach of the conditions of use (see C.38). Continuous monitoring and the possibility of disciplinary action serve to remind all users of the importance of appropriate use and the potential penalties associated with breaching these conditions. Suspected misuse of ContactPoint will result in an investigation that may lead to action taken under criminal law which can include a fine or imprisonment.

**2.19** If misuse has been established, a number of sanctions are available dependent on the severity of the misuse, and include:

- disciplinary action within a user's organisation;
- permanent deletion of the user account;
- prosecution for offences under the DPA and/or the CMA.

**2.20** Anyone who gains unauthorised access to or makes inappropriate use of ContactPoint, either directly or by intentionally facilitating others, is:

- acting in violation of ContactPoint usage policies; and
- likely to be committing an offence under the DPA and/or the CMA.

**2.21** Users of the system must ensure that ContactPoint and the information held on it is used in accordance with the Regulations, this guidance and other relevant legislation (see 1.09). The list below sets out a number of activities that are strictly forbidden when accessing ContactPoint, and is not exhaustive.

- access to and operating on information or systems to which you are not authorised, commonly called 'hacking';
- any use of ContactPoint for personal gratification, gain or malicious intent;
- accessing child records of family members, colleagues' friends or neighbours unless a professional relationship exists to provide services;
- using another user's account or credentials to gain access to ContactPoint;

- use of any techniques to bypass monitoring and/or auditing on the system;
- overwhelming ContactPoint with requests (outside the operational limits of the system) such that it will cause the system to be inaccessible to others (known as a 'denial of service attack');
- divulging of any information obtained from ContactPoint to an unauthorised third party;
- any act that contravenes ContactPoint policies or applicable legislation;
- bypassing any formal process for the provision of information when acting as a mediator;
- wilfully altering records such that it will negatively impact on the integrity of the information held on the system;
- any act of vandalism to the computer system or data e.g. the introduction of malicious software, and
- bypassing of any security controls to gain access to ContactPoint or related system resources.

**2.22** Using ContactPoint for purposes other than to support practitioners in fulfilling specific duties (see 1.09) or in a manner contrary to this guidance is likely to be regarded as misuse. For example, it is not appropriate for ContactPoint to be used to filter applications for school places, or to locate an adult suspected of tax evasion.

**2.23** **Users** - you must only access and use ContactPoint for the purposes set out in Regulations and in this guidance, and that are related to your work with children, young people and families. It is your responsibility to fully understand the implications of misusing ContactPoint and to act accordingly.

**2.24** **Local Partners' Line/Staff/Security Managers** - you must ensure that authorised ContactPoint users, whom you manage, understand that they may only search and use ContactPoint if they have an appropriate reason to do so.

**2.25** **Staff managers** - you must ensure that those you manage do not misuse ContactPoint and that you investigate any suspected misuse of ContactPoint or its data.

If you suspect a staff member is misusing ContactPoint, you must take immediate action, and inform the organisation's security manager and the ContactPoint Management Team, who may advise or take further action. You must support the ContactPoint Management Team in carrying out enquiries and investigations into potential misuse.

You should be ready to apply your organisation's disciplinary and appeals procedures, and escalate this process where necessary. In the case of serious breaches this may lead to prosecution under the DPA or the CMA.

You must record, locally, any details of the incident including any action taken, decisions and outcomes arising.

**2.26 LA ContactPoint Management Team** - you must ensure arrangements are in place to monitor and audit all use of ContactPoint within your area or organisation.

You should ensure that your staff use ContactPoint appropriately and detect and investigate suspected misuse.

Where unusual activity has been identified, you must:

- suspend the account and investigate immediately;
- where possible, notify their line/staff manager;
- take action according to your organisation's disciplinary procedures;
- escalate appropriately; and
- involve police where a serious offence may have been committed.

If you identify misuse by a ContactPoint user or are notified of misuse, you must work with the user's organisation or line manager to ensure that the correct disciplinary action is taken. This may include suspending or terminating the user's account and escalating appropriately where a serious offence may have been committed.

All such investigations must be recorded, including any reason given by the user, the outcome of your enquiry, and any decision made regarding the incident.

**2.27 Becoming a ContactPoint user**

Access to ContactPoint is restricted to those who are listed in, and fulfil all of the conditions set out in, the ContactPoint Regulations (see also BPP2 - Manage Users). Users must:

- need access for part or all of their work;
- have completed accredited ContactPoint training;
- have undertaken any other training which the LA or national partner considers appropriate; and
- have an enhanced Criminal Records Bureau (CRB) disclosure which is less than three years old (unless they are a member or an employee of a police authority, police force in England or an officer of the British Transport Police (see 2.31).

**2.28** All users must provide valid documentary evidence that they are who they say they are, and must do so face-to-face with those nominating, registering and training them. This will include evidence of residence and photographic identification (see BPP2 - Manage Users).

**2.29 LA/NP User Managers** - all users must have completed an approved ContactPoint training course based on the national training programme. They must also have received any other training your LA (or NP) considers appropriate. This should include information sharing training, so that the user understands the principles of information sharing (see C.44).

You are responsible for providing the necessary training to users from your local area, and should consider making 'refresher' training available where individuals have previously completed relevant training, such as information sharing training.

### **2.30 Enhanced Criminal Records Bureau Disclosures**

The requirement to have an enhanced Criminal Records Bureau (CRB), disclosure renewed every three years is specific to ContactPoint and does not replace existing organisational policies for non-ContactPoint users.

For new user accounts: if evidence of a current (ie less than three years old) enhanced CRB disclosure is not provided, access will not be allowed. For existing users, the user account will be suspended where a user's enhanced CRB disclosure was issued more than three years earlier and evidence of a renewed disclosure has not been provided. Applications for a new or a renewed enhanced CRB disclosure must be made in sufficient time to fulfil the conditions of access.

Members or employees of a police authority, police force in England or officers of the British Transport Police must be subject to vetting procedures equivalent to an enhanced CRB in order to access ContactPoint.

- 2.31** A judgement for suitability for access to ContactPoint may be made based on the information in an applicant's enhanced CRB disclosure. The fact that an applicant has a criminal record does not automatically make them unsuitable to have access. Certain convictions are particularly relevant when making this judgement.

In addition to any convictions which relate to offences against children, offences under the Computer Misuse Act or the Data Protection Act must be considered carefully.

The Department cannot advise whether a particular person is suitable for access; the ultimate decision must be made by the applicant's employer and the LA/National Partner ContactPoint Management Team.

- 2.32** **Users** – if you fail to meet any element of the conditions for access and/or fail to supply physical documentary evidence to verify your identity, this will prevent you from being trained and or being granted access to ContactPoint.

- 2.33** **Staff Managers/User Account Administrators** - you play a key part in nominating and judging the suitability of staff within your area or organisation that are to be given access to ContactPoint (see BPP2 - Manage Users).

You may only nominate employees of your organisation, or those engaged to provide services to your organisation, for access to

## ContactPoint.

- 2.34 LA/NP User Manager** - you will make the final decision to grant access to ContactPoint for an individual once you have judged them to be suitable and are satisfied that all the conditions for access have been met. One of these criteria is that you must have reviewed the applicant's enhanced CRB disclosure or have received written confirmation from the applicant's employer that the applicant has an enhanced disclosure which is less than three years old.

### **2.35 User Authentication**

ContactPoint requires the following user authentication for user access:

- a user name;
- a password;
- a Personal Identification Number (PIN); and
- a security token.

Furthermore, a reason for accessing a child's record will be required to perform a search or to access a child record.

### **2.36 User Access**

Authorised access can be achieved via the following three routes:

- **Secure web interface** - such as your employer's secure private network (see BPP1 – Manage Data – and BPP2 Manage Users and BPP4 – Practitioners and Mediators);
- **Adapted CMS** - such as your organisation's CMS where it has been adapted for ContactPoint use (see BPP4 Practitioners and Mediators);
- **Mediated access** - where one authorised user accesses ContactPoint via another authorised user (see BPP4 Practitioners and Mediators).

Each route is subject to stringent security verification and authentication processes.

For mediated access, details of both requestor and mediator will be recorded in the audit trail, but all activity will be recorded against the requestor (see Flowchart A.3). Mediated access is not allowed on behalf of practitioners who are not authorised users, nor should it be provided without carrying out the required authentication procedures.

Mediated access is different to 'brokered' contact with sensitive services (see 3.20) and information sharing.

- 2.37 Users** - if your CMS sends data to ContactPoint, you should not use the web interface to add or amend data on ContactPoint, unless there is an urgent and overriding need to do so (see BPP4 – Practitioners and Mediators).

### 2.38 **Suspending a user account**

The ContactPoint Management Team may decide to suspend a user account for a number of reasons, including where:

- there is prolonged inactivity of an account;
- a user is known to be going on extended leave (e.g. secondment, maternity or sickness) and has no need to use ContactPoint;
- a user has been suspended by their employer, for any reason;
- a user has left their employer and has no need to access ContactPoint;
- a user's enhanced CRB disclosure was issued more than three years earlier and evidence of renewed disclosure has not been provided;
- a user is found to be not adhering to any significant aspect of this guidance;
- an investigation into misuse of ContactPoint is being conducted, and/or;
- (potential) misuse has been identified (see 2.20)

**2.39 Users** - if you are planning to take extended leave from your current role, you should notify your line manager and/or your ContactPoint user account manager in order for them to arrange for your account to be suspended.

If your account is suspended whilst an investigation is carried out, you must assist in any investigation which is undertaken. You will not be able to access ContactPoint whilst your account is suspended, nor must you attempt to access ContactPoint .

**2.40 Staff Managers** - you will be informed when the user account of someone you manage is suspended. Account suspension does not always indicate misuse. Where potential misuse has been identified an investigation will be conducted by your own organisation or by the LA ContactPoint Management Team. You must cooperate with this investigation.

**User Administrators** - where suspicious activity has been clearly identified, a local partner user account administrator can immediately suspend an account in order to safeguard ContactPoint data. They must then notify and cooperate with the LA (see BPP2 – Manage Users).

**2.41 ContactPoint Management Team** - If one of the situations listed at 2.39 applies to a user, you must consider whether to suspend their user account. Whenever you suspend a user account you must inform the user's staff manager and, if appropriate, the user.

If you believe a user poses a particular threat to ContactPoint security you must suspend their user account. If the user is currently logged on to the system you should make a request to the National ContactPoint Team asking them to immediately disable the user's account.

You must carry out any necessary investigations as quickly as possible.

You should, where feasible, involve the user in these investigations and keep them informed of the progress and any decisions that are made. If the outcome is satisfactory, you should reactivate their account as soon as possible. A written record must be kept of all investigations and any decisions which are made (see BPP2 - Manage Users).

**2.42 Closing a ContactPoint user account**

When a user no longer needs or should no longer have access to ContactPoint, their user account must be closed.

**2.43 Users** - when you leave or change roles and no longer need access to ContactPoint, you must inform your line manager and/or user account manager and surrender your token. Attempting to access ContactPoint after this will be treated as misuse and action will be taken.

**2.44 Staff Managers/User Account Administrators** - you should notify the LA User Manager before the staff member leaves/changes role to ensure that their account is closed on the correct date. Security tokens must be returned to the user account administrator as soon as possible.

**2.45 LA ContactPoint User Managers** - You must ensure that user accounts which you administer are closed as soon as it is determined that they are no longer needed or should no longer be used. Security tokens must be recovered and safely stored and/or deactivated and cannot be used to access ContactPoint.

You must periodically review user accounts which appear to be dormant and suspend or close accounts as necessary. You may ask to view partner organisations' records and ensure that these documents are up to date (see C.01).

## **3.00 USING CONTACTPOINT**

### **3.01 Consent**

For the most part, ContactPoint will not require consent to hold the basic child records. However, consent is required in the following two situations:

- recording 'sensitive service' involvements on a child record (see 3.17); and
- maintaining a child record on ContactPoint for a participating young person aged 18 or over (see 1.10).

Many organisations and professional bodies already have procedures relating to consent for their own records. In some cases, these may need to be extended or adapted to include the situations set out above in relation to ContactPoint.

**3.02** In the two situations set out in 3.01, informed and explicit consent (see C.05) should always be sought, either from the child, where they are judged to have sufficient understanding (see C.34), or from their parent/carer.

**3.03** **Users** - there is no facility to record consent on ContactPoint. The existence of a 'sensitive service' involvement or retention of a record for a young person aged 18 or over will be based on your having secured informed and explicit consent beforehand (see Flowchart A.1).

**3.04** Consent relating to child records on ContactPoint (see 3.01), can be sought as part of your general consent seeking procedures. However, in doing so, care must be taken to ensure that any approach for consent is as transparent as possible. Consent to place or retain information on ContactPoint must never be implied, nor secured as a condition for the provision of services. Further information on consent and competency is found in the 'Information Sharing: Practitioner's Guide' (see C.44).

**3.05** Involvement of a sensitive service can be recorded or retained on ContactPoint without consent where a practitioner believes that there is reasonable cause to suspect that the child or young person is suffering or likely to suffer significant harm.

**3.06** **Users** - when seeking consent, you should:

- judge whether a child is capable of giving consent themselves (they may wish to involve their parent/carer);
- ask a person with parental responsibility to consent on behalf of the child if a child cannot consent or where you have judged that they are not competent to consent;
- explain ContactPoint, including its purpose and what is held on a child record;
- explain that contact details for any 'sensitive service' will not be visible to other practitioners and contact can only be requested through 'brokering' by the ContactPoint Management Team;

- explain that consent can be withdrawn at any point until the record is archived; and,
- confirm that this has been understood and that consent has been given to record details on ContactPoint.

You should record this agreement within your own organisation - there is no facility to record consent on ContactPoint.

**3.07 Staff Managers** - You should ensure that your ContactPoint users can explain ContactPoint, and the implications of consent, to children and/or their parents/carers. From summer 2007, materials are available to support ContactPoint users. You should ensure that your staff are aware of and have access to these materials.

**3.08 LA ContactPoint Managers** – Materials are being produced that explain the purpose of ContactPoint, including materials specifically produced for children, parents and carers. You should ensure ContactPoint users are aware of and have access to these materials.

**3.09 Withdrawal of consent**

Consent cannot be regarded as open-ended. The child, or where appropriate their parent/carer, should be asked to renew consent and may choose to withdraw consent at any time, in line with existing good practice. When consent is withdrawn the practitioner or service should amend their involvement on the child record for immediate archive.

**3.10 Users** - When consent has been withdrawn, you should immediately remove your contact details or services' involvement from the child record.

**3.11 Recording involvement**

Examples of when it is appropriate to record contact details on a child record include:

- contact between a practitioner and child/young person has resulted in case notes being made (although these notes will never be held on ContactPoint);
- the practitioner has knowledge about the child that other practitioners may find useful, or;
- the practitioner has taken action, undertaken an assessment, initiated an episode of care or made a referral to another practitioner.

**3.12 Users** - if you are working with a child or young person, it is important that your involvement is recorded on ContactPoint. This will help you discharge a number of duties, chiefly those under section 10 of the Children Act 2004 - to cooperate to improve well-being.

Placing your contact details on ContactPoint is not a substitute for taking action. Where you have concerns about a child, you must follow your organisation's existing procedures.

Placing your contact details on ContactPoint does not create a requirement for you to have to share information with other users. Such decisions must be based on professional judgement, including whether you have, or should seek, consent to share. Decisions should be supported by organisational policies and procedures, professional guidance, and information sharing training (see C.44).

**Schedule 4 Users** - (see C.37) - you are required to supply the data required by ContactPoint (see C.36), and indicate your involvement on a child record for a child/young person with whom you are working.

**Schedule 5 Users** - (see C.38) - you are permitted to supply the data required by ContactPoint (see C.36) and should indicate your involvement on a child record for a child/young person with whom you are working:

- if any of the conditions at 3.13 are met; and
- providing that consent has been given where this is required. (see 3.01).

### **3.13 Service details**

ContactPoint includes the contact details for practitioners/services which are working with a child. These practitioners/services are divided into:

- universal services;
- additional services (specialist or targeted); and
- 'sensitive services'.

### **3.14 Universal services**

For the purposes of this document and for ContactPoint a 'universal service' is one or more of the universal services defined in the Every Child Matters Green Paper (see C.43):

- GPs, health visitors, midwives and school nurses;
- early education and childcare; and
- primary and secondary education.

### **3.15 Additional services**

Where an additional service (referred to in Regulations as a 'targeted' or 'specialist service'), is being provided to a child or young person, the name and contact details for the practitioner or team leader, as a minimum should be included on the child record.

Organisations providing additional services should establish which of their activities are to be recorded as involvements, based on the criteria set out at 3.13.

Additional services may be provided in universal settings and can be indicated as such. Similarly, if any agency is providing multiple services, by multiple practitioners, and these are considered suitable for inclusion, ContactPoint will support multiple service involvements from the same agency to be indicated on a child record.

### 3.16 Sensitive services

For the purposes of ContactPoint, 'sensitive services' (see C.29) are defined as specialist or targeted services which relate to sexual health, mental health or substance abuse.

**3.17 Sensitive service users** - Before indicating their involvement, practitioners providing a 'sensitive service' should secure informed, explicit consent from the child/young person, unless in your professional judgement there is sufficient need to override consent (such as where there is reason to suspect that the child or young person is suffering or is likely to suffer significant harm).

**3.18** The nature of the service will not be visible, nor will any contact details. Instead, ContactPoint will show: "*One or more specialist and targeted services have been recorded*".

**3.19** If you are a '**sensitive service**' provider, when seeking consent (see 3.01) to add your contact details to a child record, you should have regard for the recommendations set out at 3.06.

### 3.20 'Brokering'

The LA ContactPoint Management Team will act as liaison between a ContactPoint user and a 'sensitive service' organisation or practitioner, acting only as an intermediary. The LA will not judge whether contact is appropriate - the sensitive service makes the decision whether to make contact with the practitioner who made the enquiry (see A.2).

To facilitate 'brokering', 'sensitive services' should establish which of their activities are to be recorded as involvements. This could be at an organisational team or individual staff level as appropriate.

**3.21** 'Brokering' contact only applies to sensitive services and is not to be confused with mediated access (see 2.37).

**3.22 Users** - if you need to contact a 'sensitive service', you should contact the LA ContactPoint Management Team who will 'broker' contact for you.

**3.23 LA ContactPoint Management Team** - if you are contacted by a ContactPoint user who wishes to make contact with a 'sensitive service', take note of the user's contact details, the nature and reason for the request, and pass these onto the 'sensitive services' user.

**3.24 Sensitive Service users** - If the LA ContactPoint Management Team informs you of the request to make contact with another ContactPoint user, you must consider the potential importance of the information you hold in order to decide whether to make contact.

Once you have decided whether to make contact, you must record your decision and any reasons, locally; ContactPoint will not hold such information. If you decide not to make contact, you must inform the

ContactPoint Management Team as soon as possible.

**3.25** As with all indications of involvement, the above specific indicators are not a substitute for taking necessary action, or carrying out your duties under sections 10 and 11 of the Children Act 2004, the Children Act 1989, nor other statutory duties applicable to your role.

**3.26 Additional indicators:**

In addition to indicating universal or additional service involvements, ContactPoint can also record the following involvements:

- Common Assessment Framework (CAF)
- Lead professional

**3.27 Common Assessment Framework (CAF)** (see C.04): Contact details for the practitioner(s) who has/have undertaken the most recent CAF assessment(s) can be indicated on ContactPoint. The assessment itself will not be held on or accessible from ContactPoint.

It is considered good practice to notify the child/young person and/or parent/carer that this will be indicated on ContactPoint. This can be achieved within the general CAF consent seeking process.

**3.28 Schedule 4 users** - You are required to supply data to ContactPoint. Where you are the CAF coordinator, this includes indicating that a CAF exists for a child, and your contact details.

**3.29 Schedule 5 users** - You are permitted to supply data to ContactPoint. Where you are the CAF coordinator, this includes indicating that a CAF exists for a child, and your contact details.

**3.30 'Sensitive services'** – if you work in a 'sensitive service' and have undertaken a CAF, you are able to indicate this, whether or not your 'sensitive service' involvement is recorded on ContactPoint.

If your involvement is recorded on ContactPoint the existence of your CAF assessment will not be visible to other ContactPoint users unless you indicate this separately. Contact regarding your 'sensitive services' role will still be 'brokered' via your LA.

**3.31 Lead professional** (See C.13) - a practitioner working with a child in order to coordinate provision and act as a single point of contact when a range of services are involved.

In order to support your lead professional activities, your role should be indicated and visible to other ContactPoint users.

**Schedule 4 users** - you are required to supply data to ContactPoint which includes your lead professional status.

**Schedule 5 users** - you are permitted to supply data to ContactPoint;

however, it is considered good practice to notify the child/young person and/or parent/carer that your lead professional role will be indicated on ContactPoint in order to act effectively as a single point of contact for other ContactPoint users.

**3.32** **'Sensitive services'** - if you work in a 'sensitive service' and act as a **lead professional**, you are able to indicate your lead professional role, independent of your sensitive service involvement - otherwise your lead professional status will not be visible to other ContactPoint users. Contact regarding your 'sensitive services' role will still be 'brokered' via your LA.

**3.33** **All Users** - as with all indications of involvement, the above specific indicators are no substitute for taking necessary action, nor carrying out your duties under sections 10 and 11 of the Children Act 2004, the Children Act 1989, nor other statutory duties applicable to your role. ContactPoint is simply a tool to help support you in your work.

**3.34** **Supporting continuity of service provision**  
Indicating service/practitioner involvements helps ContactPoint to support service continuity by enabling practitioners to identify practitioners and services that were working with the same child or young person in their previous location.

**3.35** **Users** - you must understand the importance of adding and updating your details on ContactPoint (either through your own CMS or via the web). This also includes where addresses have changed or families have left the area.

**3.36** **Staff Managers** - you must ensure that those you manage understand the importance of adding and updating their details on ContactPoint in order to support service continuity.

**3.37** **ContactPoint Management Team** - Responsibility for a child record is transferred automatically when a new address for the child has been supplied to ContactPoint, *and* there are no targeted or specialist services being provided. If there are targeted or specialist services involved, an agreement must be reached between the former LA and the LA where the child now lives.

If no new address is sent to ContactPoint, responsibility remains with original LA until such time as one of the conditions above is met (see BPP1 – Manage Data).

**3.38** **Ceasing involvement**  
When a practitioner or service involvement ceases, contact details will remain on the child record for one year. This is the standard ContactPoint retention period.

**3.39** **All Users** - where you have been providing a service to a child who moves away from your area, you must update the child record

accordingly. This includes indicating that your involvement has ceased and details of the child's new address where known.

**Specialist or Targeted services** - you can extend the retention of your contact details for up to five years where you judge that it would be helpful to other practitioners. When circumstances change and the extended retention is no longer justified, the extension must be cancelled and the practitioner contact details immediately archived.

**3.40 ContactPoint Management Team** - Where a child ceases involvement with all services in your LA, and may have moved to another area but not yet engaged with any services working with ContactPoint, you retain responsibility for the child record until you are able to locate the child and agree with the new LA that the responsibility for the child record can be transferred.

**3.41** When the standard or extended period of retention for an involvement with a child is reached contact details will pass into the archive. This information will not be accessible to other users and will only be accessed in a limited number of circumstances (see 4.63).

**3.42 Highly mobile children and families**

Highly mobile children and families move frequently within and between LAs. Where an authority is identified to lead on the provision of services, for example where a child from a Gypsy, Roma or Traveller family has a base school, this LA will also retain responsibility for the ContactPoint record. Where there is no identified lead authority, ContactPoint will allocate the child record to an authority, where it should remain until a more suitable authority is identified. Both authorities must agree to the transfer of responsibility for the child record.

**3.43 Looked after children**

Where an LA has social services responsibility for a child and places that child with another LA, the previous LA remains responsible for that child until an agreement is made between both LAs for the transfer of responsibility of the child record.

**3.44 Child leaves England**

When a child has left England and it is unlikely that he or she will resume residence in England during the next three years (for example when a family emigrates) ContactPoint must be updated to reflect this.

If a child has moved to an address outside England, with the intention of returning to England within three years, the child record will remain on ContactPoint. ContactPoint training sets out how this will be managed.

**3.45 Users** - If you come into contact with a child who has recently returned to England, having been out of England for more than three years but less than six, you will not be able to locate the relevant child record. You will need to contact the LA ContactPoint Management Team to allow them to

search the archive and restore the child record.

If the child/young person has been out of England for over six years, it is likely to have been deleted from the archive. You will need to create a new record either by your CMS or via the secure web interface.

### 3.46 Young people aged 18 and over

It is possible to retain records for some young people up to the age of 25 where the young person has given informed and explicit consent (see C.05). This provision only applies to records of young people who may be subject to arrangements under section 10 of the Children Act 2004 (see 1.10), and those with learning difficulties who are receiving services under the Learning and Skills Act 2000 (see C.14). This is to support the transition to adult services, particularly where a young person has complex needs. This decision should be reviewed annually on the young person's birthday.

### 3.47 Children not receiving education

There is a duty (Section 436A of the Education Act 1996) on LAs to identify children of compulsory school age in their local area who are not receiving a suitable education.

ContactPoint can help LAs discharge this duty by generating a standard report on all children in an LA area who do not have an educational setting recorded on their ContactPoint child record. This report can be run each month by the ContactPoint Management Team.

**To Note** - This report contains personal information and must therefore be treated with great care. All information printed from ContactPoint is subject to the DPA and must be held securely and destroyed when no longer required.

ContactPoint can also record where children are being educated in settings other than at school, for instance at home or in hospital.

### 3.48 Users - Where no educational setting is recorded it could be that:

- a child is receiving an education, but the educational setting has not been provided to ContactPoint; or
- the child is not receiving education.

If you are aware that the child is receiving education and this is not shown on ContactPoint you should inform the appropriate point of contact in your LA.

If you work in the LA team responsible for identifying children not receiving education, you may access the children not receiving education report generated by ContactPoint (see 3.47).

**To Note** - This report contains personal information and must therefore be treated with great care. All information printed from ContactPoint is

subject to the DPA and must be held securely and destroyed when no longer required.

**3.49 Recording date of death**

ContactPoint will record a date of death. This provides a means of minimising unnecessary or inappropriate contact with the family by practitioners. Any data source or user can notify ContactPoint of the death of a child. However, this will not be officially confirmed until the Registrar General confirms the death has been registered.

**3.50 Case reviews and enquiries**

Where it is necessary to hold a multi-agency panel, inter-agency meeting or conference, ContactPoint can be used to identify other practitioners who work with a child.

**3.51** To support statutory Local Safeguarding Children Boards (LSCBs - see C.16) in carrying out serious case reviews and investigating unexpected child deaths, ContactPoint can provide information from the child record and archive in the form of a Full Child Record Disclosure. This Disclosure will detail practitioner involvement.

**To note:** This report contains personal information and must therefore be treated with great care in line with DPA. Any information printed from ContactPoint is subject to the DPA and must be held securely and destroyed when no longer required.

## **4.00 CONTACTPOINT ADMINISTRATION**

### **4.01 Governance**

Governance of ContactPoint relates to the leadership and accountability for the operation and management of the system. It also relates to decision making processes which determine access to ContactPoint as well as its operation and use.

**4.02** The governance of ContactPoint is shared between the Department for Children Schools and Families, local authorities, and partner organisations (see C.22). The Department for Children Schools and Families is responsible for national governance of ContactPoint. At the local level, governance is managed through the initial and ongoing accreditation process between the LA ContactPoint Management Team and their local partner organisations.

**4.03** Under the ContactPoint Regulations all local authorities are under a duty to participate in the operation of ContactPoint:

**4.04 LA ContactPoint Management Teams** - you are responsible for:

- establishing a team with appropriate skills and experience to establish and operate ContactPoint;
- establishing secure local data supply agreements and ongoing relationships with local data suppliers;
- creating and managing child records, and ensuring data accuracy;
- managing and ensuring the security of ContactPoint in their local area;
- determining who in their local area should have access including managing shielded records and brokering of sensitive services contact;
- overseeing training for ContactPoint users;
- monitoring, auditing and investigating use of ContactPoint by local users;
- determining the archiving of child records;
- producing local statistics to support service planning; and
- promoting the use of ContactPoint.

**4.05 National Partners** - you are responsible for managing staff (see C.32) who access ContactPoint, including opening, suspending and closing user accounts based on the ContactPoint conditions of access (see 2.28).

**4.06** Further guidance on the roles and responsibilities of LA and NP teams is available from LARA (see C.46). LA staff responsible for the maintenance and management of ContactPoint must ensure that they comply fully with all ContactPoint specific policies and procedures.

### **4.07 Engaging partner organisations**

LAs are responsible for engaging with local partner organisations who supply data to ContactPoint and/or have ContactPoint users. Broadly,

these responsibilities are:

- **Policy** - communicating and overseeing the implementation of national policy relating to the use of ContactPoint and ensure the policy is followed locally;
- **Recruiting organisations** - identifying, engaging and recruiting organisations to work with ContactPoint;
- **Organisational accreditation** - ensuring organisations are ready and suitable to make use of ContactPoint;
- **Type accreditation** - covering specific technical requirements for each data source connected to ContactPoint, including data quality; and
- **Monitoring and auditing** - ensuring that ContactPoint is properly and appropriately used.

#### **4.08 Local data sources**

These arrangements can only be made with a person or accredited body 'required' or 'permitted' to supply information, under Section 12 of the Children Act 2004 and Schedules 4 and 5 of the Regulations. An LA can engage and terminate a data source based on the Accreditation conditions.

#### **4.09 Accreditation**

Accreditation (see C.01) covers a set of processes, including audit and inspections within the children's services inspection framework, which ensure nationally that LAs, their local partners and national partners are working together to maintain agreed standards under ContactPoint's regulatory, security and operational requirements.

- 4.10** Specific role responsibilities are set out in the ContactPoint accreditation document. A senior responsible person (a director, chief executive officer or equivalent) from each local partner will need to sign up to the accreditation agreement.

Accreditation also provides assurance to the Secretary of State and the public that those involved in ContactPoint are subject to appropriate supervision, monitoring and controls.

- 4.11** In the majority of organisations, many existing policies and processes require little more than minor amendments in order to meet the ContactPoint accreditation conditions. In some cases new policies or processes may be necessary (e.g. managing security tokens).

- 4.12** All organisations are subject to a three-year cycle of re-accreditation. Re-accreditation also occurs where organisations change, processes are revised, systems are upgraded or where system usage or data quality are in variance with agreed thresholds.

- 4.13** All organisations must:
- have sufficient internal audit, control and HR functions in place;
  - be aware of the requirements and conditions set out in the Regulations, this guidance and Accreditation documents;
  - have in place processes to conduct compliance checks, take action and report/record outcomes;
  - show evidence of audit planning, inspection and follow-up action, and
  - nominate an individual or post responsible for ensuring these conditions are met.

**4.14** **Local Partner User Administrators/Line Managers** - the accreditation agreement exists between your senior responsible officer (see 4.10) and the LA.

**4.15** **LA ContactPoint Management Teams** are responsible for overseeing and supporting accreditation of local partner organisations within their own local area, acting as a lead LA (sponsor), for cross-border organisation accreditation, user management and continued assurance that providers and users are using the system appropriately. You must support local partner organisations throughout the initial accreditation process and at each re-accreditation process.

**NPs** - organisations, mentioned by name in Regulations, are responsible for determining who in their organisation may use ContactPoint and for the management of those users.

**4.16** **Engaging Local Data Sources**

These arrangements can only be made with a person or accredited body 'required' or 'permitted' to supply information, under Section 12 of the Children Act 2004 and Schedules 4 and 5 of the Regulations. An LA can engage and terminate a data source based on the Accreditation conditions. Further support is available from LARA.

**4.17** **LA Data Managers** – You should regularly review all local data feeds to identify any data supply issues. You must work with local data sources to resolve these issues. If they cannot be resolved, you must decide whether it is necessary to suspend or terminate a local data feed from ContactPoint.

**4.18** **Local partner user administration**

Local authorities can allow local or regional partner organisations to administer user accounts for their staff or those engaged to provide services to the organisation. This includes nominating staff for user accounts, managing security tokens, maintaining user account information and auditing usage.

The broader conditions for access to ContactPoint (see 2.28), remain unchanged.

- 4.19 LA ContactPoint Managers** - You are responsible for determining that individuals nominated by partner organisations are eligible for access, including user administration rights (see BPP2 – Manage Users).

You must continually monitor ContactPoint usage to identify and investigate any suspicious use or potential misuse (see 2.19).

Where you believe that misuse or unauthorised activity is being carried out by users administered by a local partner organisation, you must immediately suspend their user accounts. You must work with the partner organisation who must carry out an investigation and take appropriate action (see BPP2 - Manage Users).

**4.20 Fair Processing Notices**

Fair processing notices (FPNs) provide information to people whose data is held on ContactPoint. They should signpost people to further information. In line with the DPA, all data controllers for ContactPoint need to issue FPNs.

**4.21 Subject access requests**

Individuals have the right to request access to any personal data which an organisation which controls the data holds about them (Section 7 of the Data Protection Act 1998). This is known as a 'subject access request' (SAR). In the case of information held in a ContactPoint record, LAs will take the lead in responding to local SARs made in relation to ContactPoint (see 4.23 and BPP1 - Manage Data).

- 4.22** A SAR can only be made by or on behalf of the individual to whom the personal data relates and must be made in writing (see Flowcharts A.4 & A.5). It may specifically refer to ContactPoint or may be a broader request which can include ContactPoint data. The address for LA SAR enquiries should be suitably publicised and sample wording should be made available to help in making such requests.

- 4.23** Local authorities have established procedures for handling SARs (for other purposes). In most local authorities there will be a Data Protection Officer who is responsible for ensuring these procedures are followed. These procedures should be followed for requests relating to information held on ContactPoint. The DPA contains a number of exemptions where such personal data should not be released - these should also be considered when deciding whether to disclose details from ContactPoint. Take care to ensure that this process is not abused by an estranged parent trying to track down a child (see 4.29).

**4.24 Correcting information**

Having made a SAR, a data subject or their representative may identify inaccurate or incomplete information on their record. If the LA is satisfied that the information is inaccurate or incomplete, then it must amend the record (see BPP1 - Manage Data).

**4.25** Whilst a child record is the responsibility of the LA to which it has been allocated, responsibility for the accuracy of the source data lies with the organisations which send the data to ContactPoint. The data subject may wish to take up any outstanding or unresolved discrepancy with the source system responsible for sending this disputed data to ContactPoint.

**4.26 Disputed Data**

If after reasonable efforts have been made, data still exists on ContactPoint which cannot be changed to the Child's/young person's or parent's/carer's satisfaction, it becomes 'disputed data' and can be indicated on ContactPoint as such. However, the details of any dispute should be recorded locally - ContactPoint will not hold details of any dispute because this may contain case data (see BPP1 - Manage Data).

**4.27 Users** - You should explain ContactPoint to children and parents/carers, including what is held on a child record. However, this does not mean that you can show them what you see on your screen. You should make clear that they have a right of access to their information via a SAR.

If you receive a SAR relating to ContactPoint you should forward this to your ContactPoint Management Team. If the request relates to information held in your organisation's files, and does not include ContactPoint data, this should be answered in line with your own organisation's existing policies. Advice on handling such requests should be sought from your manager or Data Protection Officer.

**4.28 Staff Managers** - You should help those you manage to identify whether a SAR relates in part or wholly to ContactPoint or to the data your organisation holds. SARs which do relate to ContactPoint should then be directed to your ContactPoint Management Team.

**4.29 LA ContactPoint Management Team** - You must follow your established process for handling SARs, consulting your Data Protection Officer and legal advisors as appropriate. When it has been decided that information from ContactPoint should be released in response to a SAR, you should produce the 'Full Child record Disclosure'.

If the data subject identifies inaccuracies or out of date information in the record that can be disproved, you should take reasonable steps to amend the child record. This will lead to notifications being sent to source systems that their information does not match that held on ContactPoint.

In the case of complaints relating to SARs or requests under the Freedom of Information Act, these should also be managed by the Data Protection Officer or the LA in line with existing procedures.

**4.30 Freedom of Information Requests**

Requests made to LAs under the Freedom of Information Act (FoIA) 2000 (see B.11), relating to ContactPoint use or data in their area will be

handled by the LA concerned via existing policies and procedures. Requests which relate to the national or regional operation of ContactPoint should be passed to the national team.

The FoIA does not cover data held on ContactPoint for individuals - this falls under the Data Protection Act 1998.

#### **4.31 Complaints**

As part of the accreditation conditions, all local and national partner organisations must have in place effective complaints procedures already and must manage complaints where they relate to their own staff and data handling procedures.

**4.32** Complaints relating to the use of ContactPoint by LA staff, including those within the ContactPoint Management Team, should be managed through the existing LA complaints and review process. Where a complaint is received for which an LA is not responsible (e.g. a local partner), this should be directed to the appropriate local partner organisation or body.

**4.33** In the case of complaints relating to Subject Access Requests or requests under the Freedom of Information Act, these should be managed by the data protection officer in line with existing procedures.

**4.34 Local Partner User Administrators** - you must ensure that there are arrangements in place within your organisation to manage complaints about your staff who use ContactPoint or the data you supply to ContactPoint.

**4.35 ContactPoint Management Team** – you must ensure that there are arrangements in place to cooperate with your organisation’s customer service team in line with your existing complaints procedures.

Local authorities must include information about their complaints procedure in materials they produce to promote and explain ContactPoint.

#### **4.36 Shielding records**

ContactPoint has the facility to hide or ‘shield’ data from ContactPoint users. This is principally intended to prevent the whereabouts of a child being identified either through:

- visibility of the address details from ContactPoint, or;
- ContactPoint providing enough information for a likely whereabouts to be deduced (e.g.: a service address).

In order for the system to work effectively and for children and young people to receive the benefits offered by ContactPoint, a shielded record will only show the ContactPoint unique identity number, the child’s or young person’s names, their gender and their date of birth.

**4.37** Determining whether to protect a child’s whereabouts by shielding a child record can only be done by an LA which is under a duty to consider the

views of the person to whom the record relates, the views of their parent/carer and of any Schedule 4 or 5 body involved with the child or young person (see Flowchart A.6).

**4.38** It is vital that shielding (and thereby disclosing the whereabouts of a child or young person) is only applied where there are strong reasons, for example, where a practitioner has reason to believe that not doing so is likely to:

- place a child at increased risk of significant harm;
- put a child's placement at risk (in the case of adoption);
- place an adult at risk of significant harm, and/or
- prejudice the prevention or detection of a serious crime.

**4.39** Such cases could arise for example where:

- a child/young person is adopted where there is little or no contact with birth parent(s) or wider family members;
- a child/young person and/or their parent/carer, are fleeing abuse or domestic violence; and/or
- a child/young person and/or their parent/carer or family member are subject to police protection.

The need to shield a record may also arise for children/young people and or their parent/carer in a very limited number of unique circumstances not covered by these categories, for example, siblings or co-habiting children and young people. The necessity to shield a record must therefore be assessed on a case-by-case basis.

**4.40** Practitioners will identify cases in which the whereabouts of a child should be protected either in light of their own knowledge of a child/young person and/or their parents, wider family or carer(s), or because concerns are raised by family or carer(s).

**4.41** To ensure that the shielding facility is used and managed appropriately, the LA ContactPoint Management Team should undertake an initial review within seven days of the shield being requested, to determine whether or not the record should be shielded. Periodical reviews of the shielded record should be undertaken every six months thereafter. These reviews should seek views from the child/young person, their parent/carers and any relevant involved practitioners.

**4.42** LA ContactPoint managers can un-shield records only where all data sources or services no longer request that a record requires shielding.

**4.43** **Users** - In order to help you assess whether the child/young person's or their parent/carer's request to shield a child record are legitimate and to address their concerns appropriately, you may need to explain the following:

- the differences between shielding and sensitive services;
- the reasons why records are shielded, and
- the potential disadvantages of shielding records on ContactPoint

You may also wish to consult any lead professional and/or other practitioners involved with the child/young person, as well as their own line manager, for more information and/or professional advice.

You must act promptly if you have strong reasons to believe that a record needs to be shielded (see 4.38 for examples). You should discuss this, where appropriate, with the child and/or their parent/carer. It is not appropriate to simply shield a record where there is an opposition to ContactPoint in principle.

You should also discuss your decision with your manager before making a shielding request, wherever this is possible.

Where appropriate, you should also consider the safeguarding of family members and/or co-resident children/young people as the records for these individuals may also need to be shielded. You should also consider whether it would be useful for other practitioners to know that you are 'shielding' the record on ContactPoint.

Practitioners who are users can send a shielding request to the LA ContactPoint manager where they judge that a child record must be shielded.

To ensure that shielding is only applied where appropriate, the LA ContactPoint Management team will review the shielding requests it receives and remove the shields when necessary.

To limit the cases in which a child record is left shielded unnecessarily, you should advise the LA ContactPoint Management Team when, in your professional opinion, a shield is no longer required.

**4.44 Line Managers/User Administrators** - you will be responsible for the shielding requests made by your staff, and should discuss the appropriateness of shielding a child record on ContactPoint with those you manage. You should be prepared to support your staff in considering the continued need for shielding, when this is reviewed.

**4.45 LA ContactPoint managers** – you have the facility to run a report which highlights when a shielding request has been submitted by an authorised user.

You may also be contacted directly by practitioners who do not have access rights to 'shield' a child record or, in rare circumstances, by a child/young person or parent/carer. Where a request to shield a child record is made to your team, from a practitioner who is not a user or a child/young person or their parent/carer, the request should be dealt with as a matter of urgency. You should shield the record immediately and then review whether the shield should remain, taking into account the views of the child/young person or their parent/carer, and those of

practitioners working with the child or young person.

You should review all shielding requests within seven days to determine whether there are strong reasons for the shield to be applied.

You should periodically review shielded decisions every six months, starting six months after the shield is first applied to determine whether the shield should remain. Again, this review should take into account the views of the child and/or their parent/carer, and of practitioners who work with the child or young person, particularly those who have requested shielding.

ContactPoint will not hold any details of the shield - you should keep a log of shielding requests and decisions as part of the shielding review.

#### **4.46 Access to shielded records**

In order to ensure that ContactPoint does not inadvertently confirm or indicate the whereabouts of a child or young person with a shielded record, a practitioner will only be able to find a child record by inputting information that is visible on a shielded record. No records will be returned if a search is made using information from any non-visible field.

**4.47** If a shielded record is returned as part of a search, the shielded record will only show minimal information, and none which will identify the child's whereabouts (see 4.36).

**4.48** LA ContactPoint Management teams will have access rights to view hidden information on shielded records so they can, where there are child protection concerns, 'broker' contact (see Flowchart A.7), between users working with the same child. No other users will have access rights to hidden information on shielded records (apart from those with 'emergency shielding override' rights see 4.52.)

**4.49 Users** - When any authorised user wishes to access information from a shielded record, they will make a request for disclosure to the LA ContactPoint Management Team member with the appropriate access rights (see Flowchart A.7).

**4.50 ContactPoint Management Team** - Given that the decision to disclose information from a 'shielded' record is a professional judgement, you should contact a practitioner involved with the child/young person (involved practitioner) when approached by a practitioner. That involved practitioner can use existing safeguarding procedures to decide whether to release information.

#### **4.51 Subject Access Requests to a Shielded record**

Information should only be released with extreme caution. Even confirming the correct spelling of a child's name may confirm the whereabouts of a child. Such decisions need to be made on a case-by-case involving the LA Data Protection Officer, taking into account the

requestor's identity and the nature of the shielding decision and the views of any practitioners working with the child.

#### **4.52 Emergency shielding override**

Provision has been made in legislation for some users to have emergency shielding override rights. This access will be restricted to child protection workers such as police officers or social services duty workers where gaining access to information held in ContactPoint may help inform their decision about the appropriate action to take or which practitioners to talk to. Invoking the emergency shielding override will immediately trigger an investigation into the reasons for doing so.

#### **4.53** Examples of when such access might be required includes:

- when a multi-agency meeting or risk assessment is needed (MARAC);
- to fulfil legislative requirements or the functions of (say) the LSCB;
- A&E attendance;
- serious illness/accident;
- 'missing' child;
- 'found' child;
- a review carried out under s.47 of the Children Act 1989;
- serious case review;
- child death enquiry, and
- an investigation of a crime toward or by the child/young person.

#### **4.54** The user with the appropriate access rights will only be able view the information on the 'shielded' record during the time period when they have logged into ContactPoint and elected to access a shielded record. If another user searched for the child record, the record would still appear to be 'shielded' to them. Invoking the emergency shielding override will immediately trigger an investigation into the reasons for doing so.

#### **4.55 Users** - If you need to access a 'shielded' record out-of-hours, you may invoke the emergency shielding override and the hidden details will be available to you for this one time only. No other ContactPoint users will be able to access the non-visible data in a shielded record unless they too invoke the emergency shielding override function.

You must assist the investigation which follows and be able to explain your reasons for accessing the 'shielded' record.

#### **4.56 ContactPoint Manager/User Manager** – If a shielded record has been accessed you must immediately begin an investigation in order to confirm the legitimacy of the action. At the start of the review you should contact the manager of the user who has invoked the emergency shielding override to find out whether the access to the record was appropriate.

You should also contact the practitioners/organisation who initially requested the shield, so that the necessary safeguarding/child protection

procedures are initiated.

#### **4.57 New identities**

There are a small number of circumstances where it is necessary for a child to be given a new identity. The police, a court, social services or other suitable bodies may decide that a new identity is necessary to protect the child from harm.

**4.58** In such cases it must not be possible for ContactPoint to make a link between the previous identity and the new identity. This can be done by immediately moving the child record for the previous identity to the archive and then creating a new child record using the new identity.

**4.59 Users** - You must not attempt to use ContactPoint to discover details of a new identity for a child or their previous identity.

If your service is involved in giving a child a new identity, in circumstances where links must not be made with the child's previous identity, you should inform the ContactPoint Management Team.

**4.60 LA ContactPoint manager** – You are responsible for managing records associated with a child's previous identity. You may also be asked to establish a new child record for the new identity. You should ensure that the record for the child's previous identity is moved to the archive before the new child record is created, and that appropriate measures are taken to prevent subsequent data relating to the former identity being matched and added to the new identity (for example as an alias or alternative address).

#### **4.61 The archive**

Information is held in the archive for a period of 6 years from the date on which it was archived, after which it will be permanently deleted. This period of retention can be extended in cases where there is a) an investigation under section 47 of the Children Act 1989; or b) under the Local Safeguarding Children Boards Regulations 2006, an exercise by an LSCB of its serious case review functions or its functions relating to child deaths. Information in the archive can only be accessed by the national ContactPoint team and the LA ContactPoint Management Teams.

#### **4.62 Closing and archiving records**

Entire records are closed and moved to the archive when:

- a child who is not a "participating young person" (see 1.10) reaches the age of 18;
- a participating young person reaches the age of 25 or withdraws consent to information being kept on a child record, whichever is the earlier;
- an LA responsible for a child's record (or the Secretary of State) becomes aware that a child is no longer ordinarily resident in England and it is unlikely that the child will return within three years of leaving;
- the first anniversary of the death of a child;

- a child is given a new identity which must not be linked to the previous identity (such as those adopted where there is little or no contact with birth parent(s) or wider family members).

#### 4.63 Retrieval from the archive

Archived records can be retrieved by the LA ContactPoint Management Team for a limited period or they can be restored to the live system and made visible to authorised users so long as they still exist, for example:

- where a child record was archived when they left England, but the child returns to England and the child is under 18 or is a participating young person;
- when access is required by or under an enactment, by a rule of law or by a court order (this covers Subject Access Requests made under the Data Protection Act 1998);
- for the prevention or detection of crime;
- for the prosecution of offenders;
- for a section 47 investigation (see B.08);
- for serious case reviews and unexpected child death investigations, carried out by a Local Safeguarding Children Board;
- for the investigation of a complaint arising out of ContactPoint operation.

**4.64 ContactPoint Manager** – You must only access or restore records from the archive in the circumstances listed above. Whenever you access the archive the reason for access will be recorded.

Where a record is the subject of an ongoing investigation (see 4.63), you may extend the period of retention beyond the six year limit. The extension should only apply until you have established whether information from the archived record is required for the investigation. Once the information is produced, you have confirmed no further information is required or the investigation is complete the record should be permanently deleted.

#### 4.65 Record-Keeping

Accreditation also requires all organisations to provide assurance that they have sufficient knowledge of and control over staff using ContactPoint, including:

- staff records (for up to six years);
- a staff handbook (covering, for example appropriate use, security awareness and information sharing).

#### 4.66 Monitoring, Audit and Inspections

As part of the continuous accreditation process, monitoring and audit should be carried out at three levels (see Accreditation C.01):

- **Partner Organisation** - ensuring their use of ContactPoint is subject to internal monitoring and audit controls;
- **LA User Manager** - responsible for determining who, from the partner organisation, may use ContactPoint;

- **'Sponsor' LA:** responsible for an organisation's accreditation and compliance.

**4.67 LA ContactPoint Managers** - You are responsible for ensuring that all activity by users in your area is audited and monitored, and that swift action is taken when non-compliance is identified.

In case of serious systemic and /or material concerns with the organisations involved, this activity may suspend or revoke the use of ContactPoint by a local partner organisation. Such action may involve:

- issuing a final warning to the organisation's senior management asking them to comply with accreditation conditions or to have their account revoked;
- suspending non-compliant parts of the organisation;
- deciding if legal sanctions need to be pursued including any police involvement;
- recording the basis of any decisions made and outcomes reached.

**4.68** Audit logs must be protected to ensure that any personal information contained within them is safeguarded.

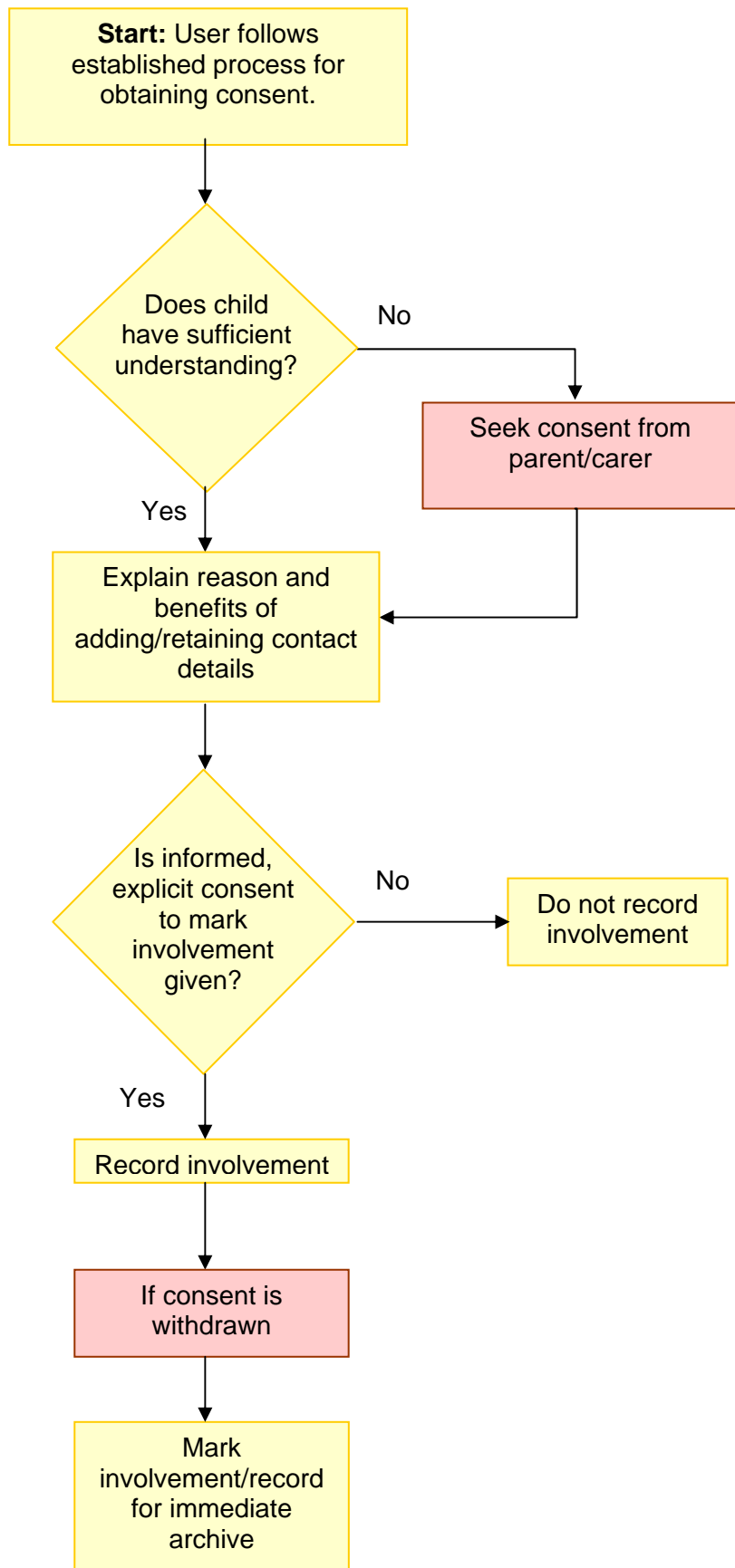
**4.69 Reporting and management information (MI)**

Apart from the 'children not receiving education' reports, Subject Access Reports and certain MI Reports information from ContactPoint should not be printed out. This includes screen prints. Doing so may pose a security risk and may be regarded as misuse (see 2.19). All information printed from ContactPoint is subject to the Data Protection Act and must be held securely and destroyed when no longer required.

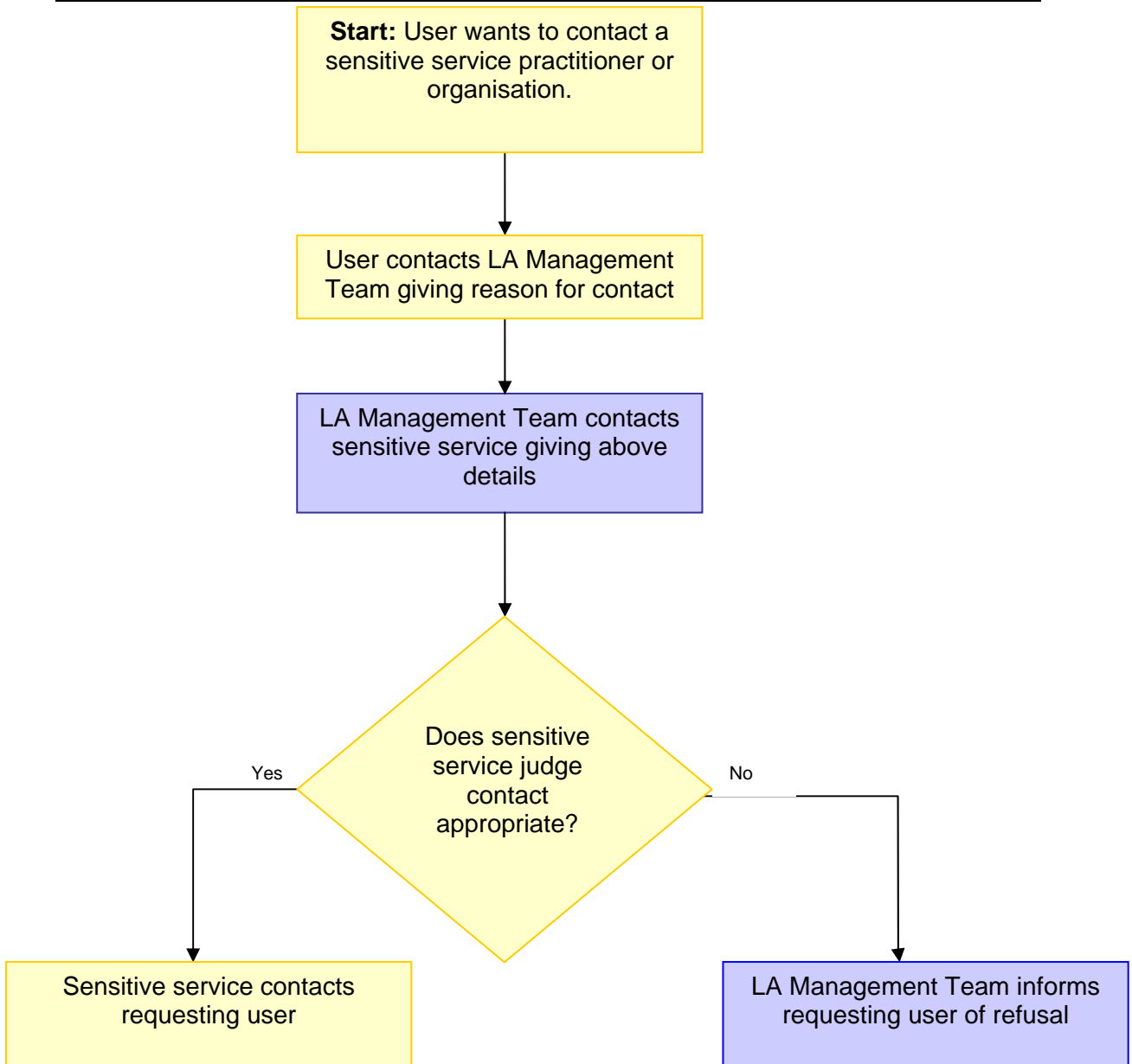
**4.70 User account administrators** – You should use the appropriate reports to support your responsibilities for reviewing ContactPoint usage. This includes regular reviews of the ContactPoint audit trail to identify and follow up any possible misuse (see 2.19).

**Data administrators** – To support the ongoing assurance of data quality, you should use reports to support your management of ContactPoint data. Where you are permitted to print or download specific reports you must ensure that these are handled securely, in accordance with the Data Protection Act, and are destroyed when they are no longer needed.

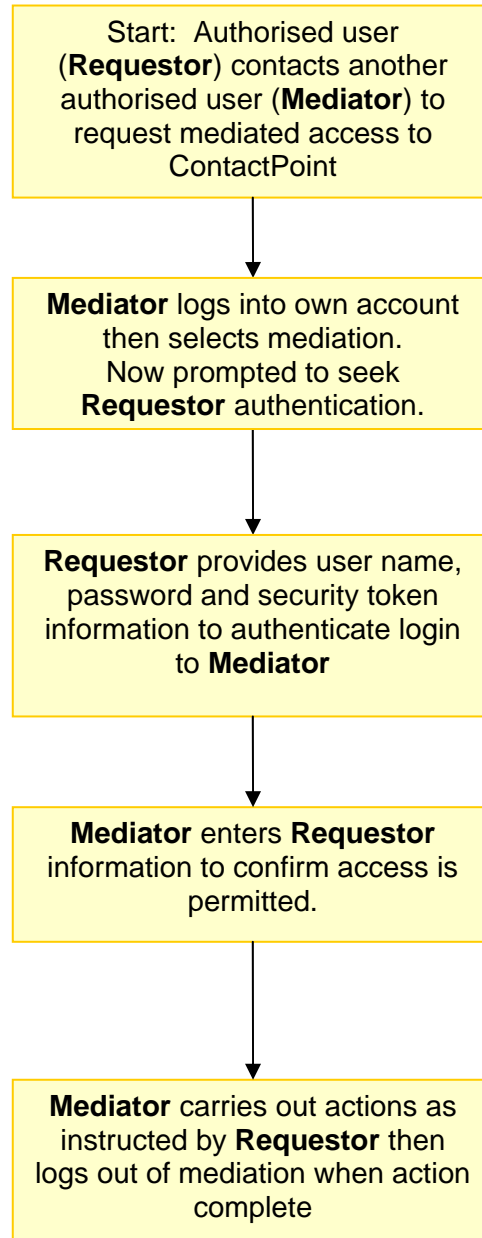
**A.1 Consent (Retaining a child record above 18 or Indicating 'Sensitive Services') (See 3.01-3.08)**



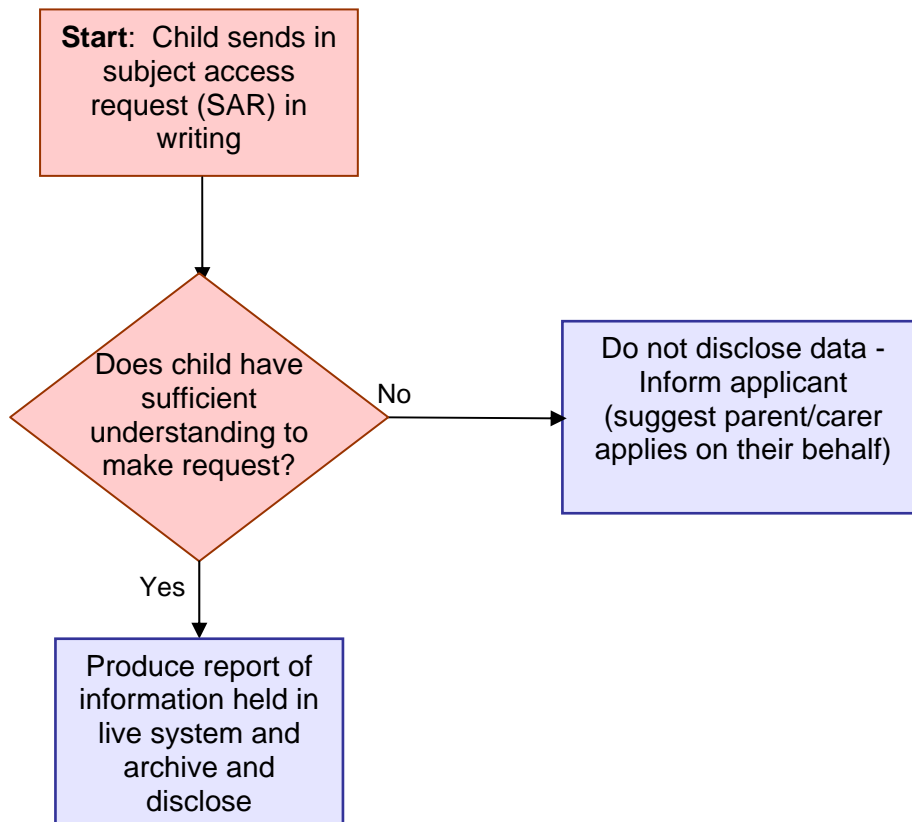
**A.2 Brokering Contact Between Users and sensitive services (See 3.22-3.26)**



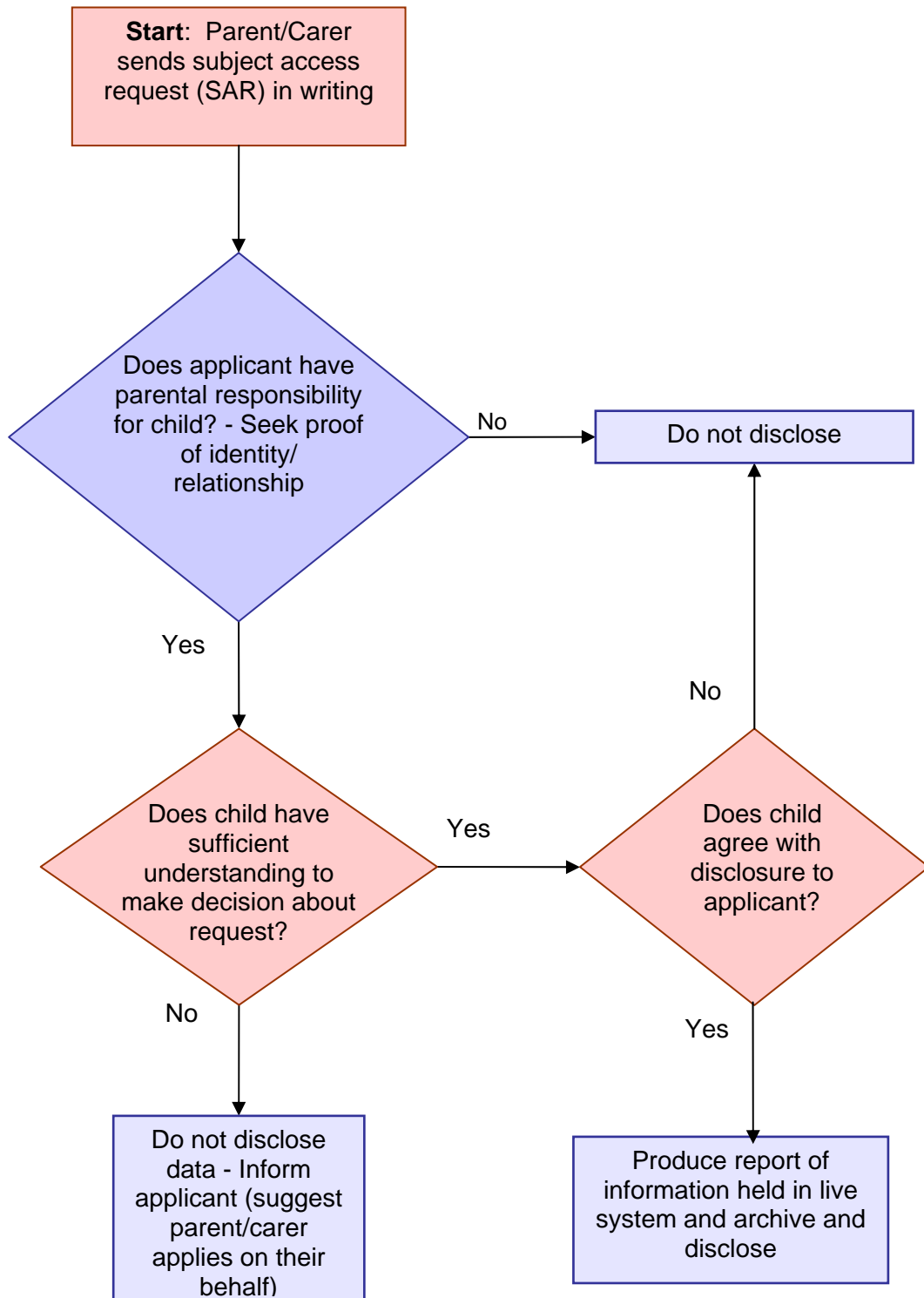
## A3 Mediated Access (See 2.37)



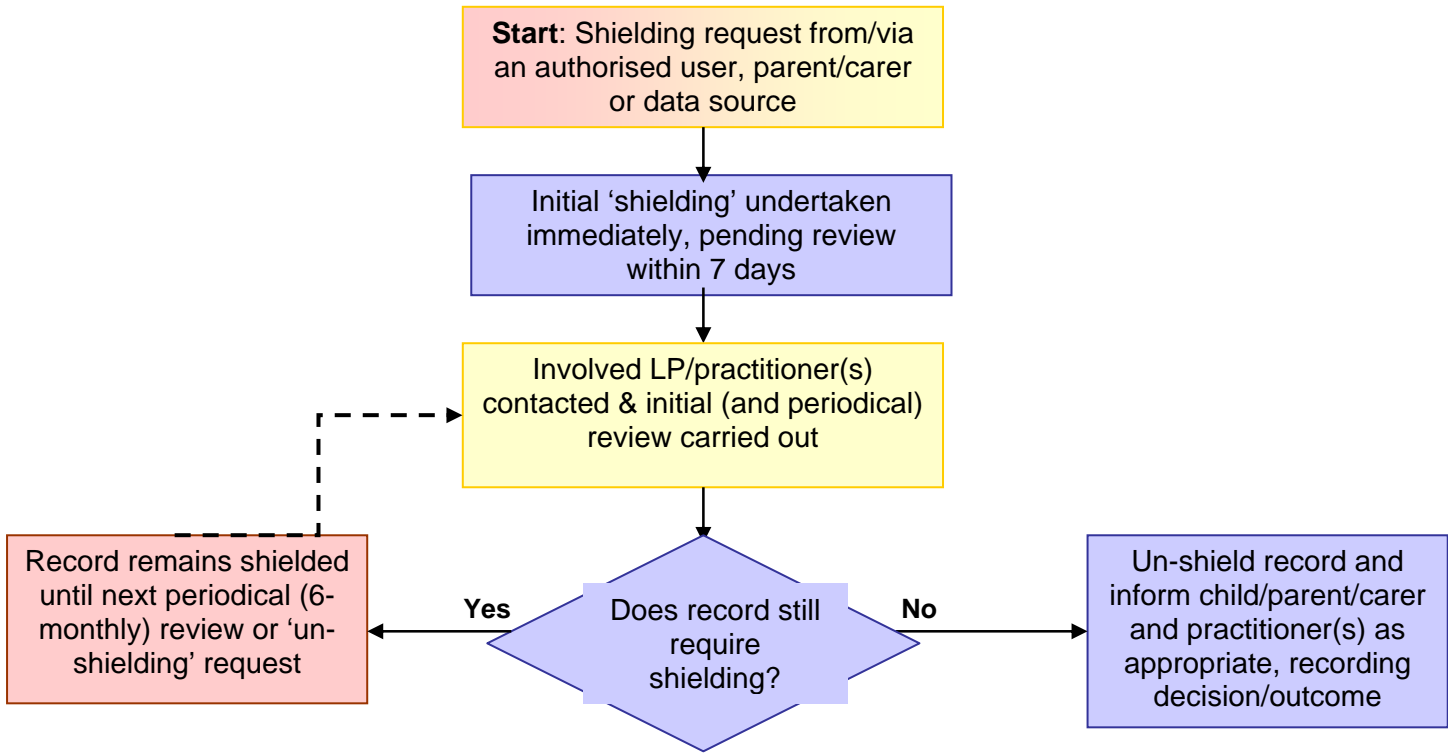
**A.4 Subject Access Request by Child (See 4.18-4.29)**



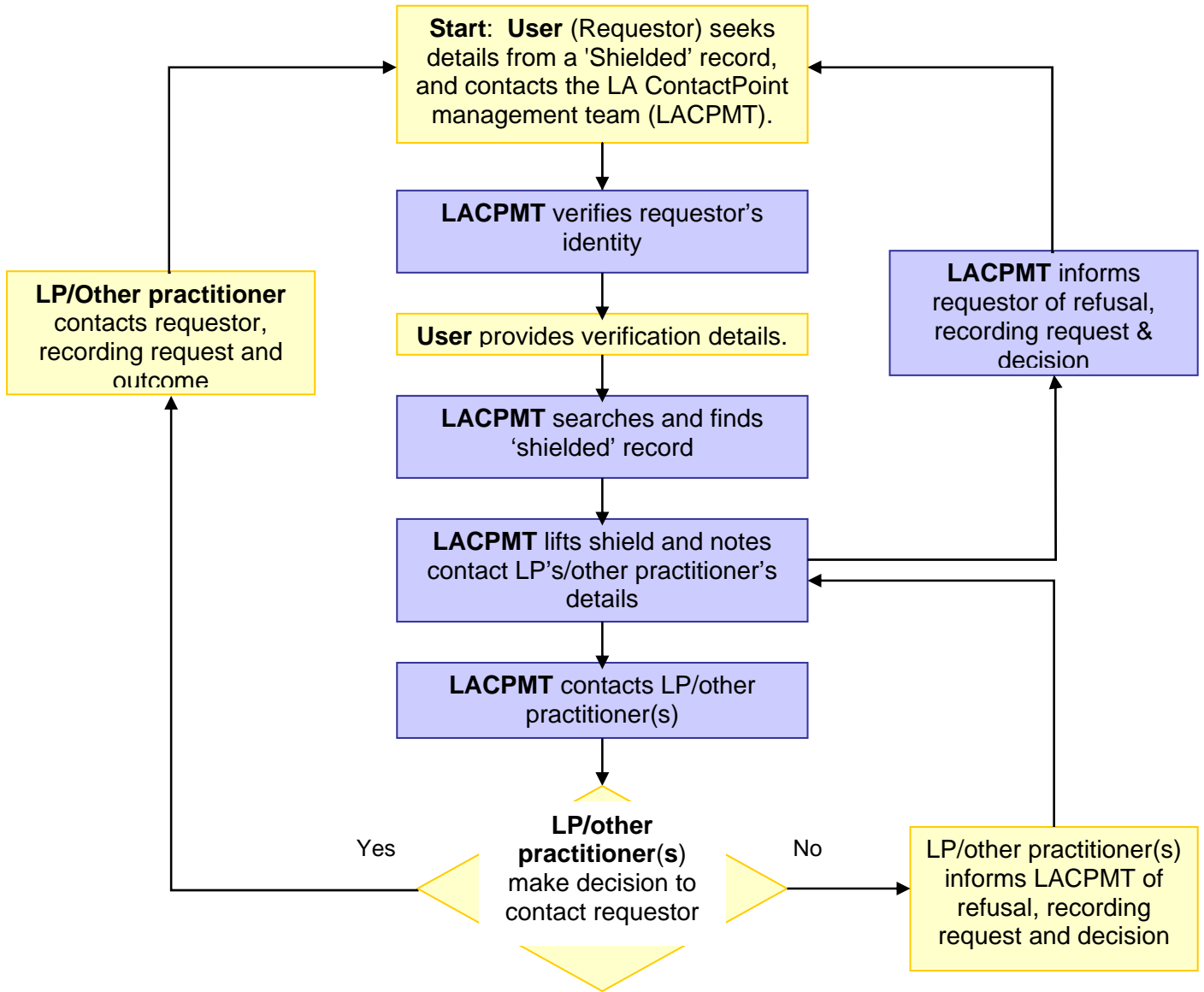
**A.5 Subject Access Request on behalf of a Child (See 4.18-4.29)**



**A.6 Shielding Records (See 4. 36-4.55)**



**A.7 'Brokering' Contact for a 'Shielded' Record See 4.49-4.50**



## **B LEGISLATION**

### **B.01 Children Act 2004**

([http://www.opsi.gov.uk/Acts/acts2004/pdf/ukpga\\_20040031\\_en.pdf](http://www.opsi.gov.uk/Acts/acts2004/pdf/ukpga_20040031_en.pdf) )

**Section 12** of the Children Act 2004 provides for the establishment and operation of a database for the purposes of arrangements under sections 10 and 11 of the Children Act 2004, or under section 175 of the Education Act 2002, and applies to England only.

### **B.02 The Children Act 2004 Information Database (England) Regulations**

**2007** ([http://www.opsi.gov.uk/si/si2007/uksi\\_20072182\\_en\\_1](http://www.opsi.gov.uk/si/si2007/uksi_20072182_en_1)), made under the Children Act 2004 Section 12, set out:

- The duty on local authorities to participate in the operation of ContactPoint;
- the information to be included on ContactPoint;
- the procedures for ensuring accuracy of the information held;
- the persons or bodies required or permitted to disclose information to ContactPoint;
- the types of users who may be granted access to ContactPoint;
- the conditions of access; and
- the length of time information can be retained on ContactPoint.

### **B.03 Children Act 2004**

**Section 10** imposes a duty on each children's services authority in England to make arrangements to promote co-operation between itself and relevant partner organisations to improve the wellbeing of children in the authority's area in relation to:

- physical and mental health and emotional wellbeing;
- protection from harm and neglect;
- education, training and recreation;
- the contribution made by them to society;
- social and economic wellbeing.

### **B.04 Section 11** imposes a duty on each children's services authority in England and other key people and bodies to make arrangements to ensure that:

- they discharge their functions having regard to the need to safeguard and promote the welfare of children; and
- any services provided by others on behalf of those under the section 11 duty are provided having regard to that need.

Section 11 statutory guidance states that arrangements should ensure that:

- all staff in contact with children understand what to do and the most effective ways of sharing information if they believe a child and family may require targeted or specialist services in order to achieve their optimal outcomes;
- all staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including

those children suffering or at risk of significant harm.

**B.05 Education Act 2002**

**Section 175** imposes a duty on local education authorities to make arrangements to ensure that their functions are exercised with a view to safeguarding and promoting the welfare of children. Similarly, governing bodies of maintained schools and further education institutions are under a duty to make arrangements to ensure that their functions relating to the conduct of the school, or institution, respectively, are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school, or who are receiving education or training at the institution.

**B.06 Section 436A of the Education Act 1996** imposes a duty on local education authorities to identify children not receiving education. It requires all local education authorities to make arrangements to enable them to establish (so far as it is possible to do so) the identities of children in their area who are of compulsory school age but who are not registered pupils at a school and who are not receiving a suitable education otherwise than by being at school. See *Statutory Guidance for local authorities in England to identify children not receiving education* <http://www.everychildmatters.gov.uk/resources/ig00202/>

**B.07 Other relevant legislation**

There are a number of further pieces of legislation relevant to ContactPoint. It is important that you understand your responsibilities when using ContactPoint. To support this, legislation will be covered in ContactPoint training and should be supplemented by your organisation's own training procedures.

**B.08 Children Act 1989**

**Section 17** - Provision of services for children in need, their families and others – it is the general duty of every LA to safeguard and promote the welfare of children within their area who are in need; and, so far as is consistent with that duty, to promote the upbringing of such children by their families, by providing a range and level of services appropriate to those children's needs.

**Section 27** – This provides that a LA, may, for help in the exercise of its statutory functions, request the help of any LA, local education authority, local housing authority, health authority and any person authorised by the Secretary of State. Those requested must comply if the request is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions.

**Section 47** - LA's duty to investigate – this section provides, amongst other things, that where a LA has reasonable cause to suspect that a child who lives or is found in their area is suffering, or is likely to suffer, significant harm, the authority shall make, or cause to be made, such enquiries as they consider necessary to enable them to decide whether they should take any action to safeguard or promote the child's welfare.

### **B.09 Computer Misuse Act 1990**

[http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1)

This Act provides that, amongst other activities, unauthorised access, facilitating unauthorised access for another person, or attempted unauthorised access to a program or data held on a computer or computer system such as ContactPoint, is an offence.

The penalties for an offence under the Act are imprisonment for up to 5 years and a fine of up to level 5 on the standard scale (currently £5,000).

### **B.10 Data Protection Act 1998**

The DPA is the main piece of legislation regulating the handling of personal information, such as that held on ContactPoint. It is built around a set of enforceable rules of good practice - the data protection principles. These principles require the fair and lawful processing of personal information and also cover data quality and security.

The DPA also gives a set of rights to individuals. These include a legal right of access to personal information. Individuals may also request that incorrect information be put right.

The DPA also provides that an offence is committed where personal data is unlawfully obtained or disclosed without the consent of the data **controller**. Committing this offence makes a person liable, on summary conviction, to a fine not exceeding the statutory maximum (currently £5,000) and, on conviction on indictment, to a fine.

The DPA is overseen by the Information Commissioner, an independent regulator who answers to Parliament. The Commissioner gives advice about compliance with the DPA and handles complaints from individuals who have concerns about their personal information. He has enforcement powers that can be used to ensure that personal information is handled in compliance with the DPA.

### **B.11 Freedom of Information Act 2000**

The Act establishes a legal right for any person to make a request to a public authority to have access to information held by that authority. This does not relate to personal information held on ContactPoint which falls under the DPA.

### **B.12 The Human Rights Act 1998 and the European Convention of Human Rights**

Article 8 of the European Convention on Human Rights (incorporated into UK law by the Human Rights Act 1998) recognises a right to respect for private and family life. Article 8.1 provides that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8.2 provides that 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 of the economic well-being of the country, for the prevention of disorder or crime, protection of health and morals or for the protection of rights and freedoms of others.

**B.13 Further legislation** such as the Police and Criminal Evidence Act 1984 (and accompanying guidance (<http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro/>), and the Regulation of Investigatory Powers Act 2000 ([http://www.opsi.gov.uk/acts/acts2000/ukpga\\_20000023\\_en\\_1](http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1)), apply as they do generally to information processing systems.

## C GLOSSARY AND REFERENCE

C.01 **Accreditation** - There are three main accreditation schemes:

- **Organisational Accreditation** - ensures that those using the system must do so under a set of common rules, and that no organisation may connect to ContactPoint, or remain connected, unless they comply with these common rules.
- **Type Accreditation** - verifying that an organisation's CMS has been properly modified to integrate with ContactPoint;
- **Instance Accreditation** - verifying that the system has been properly installed and configured,

C.02 **Best Practice Processes (BPP)** - The purpose of the ContactPoint BPP is to provide Local Authorities, national and local partners with a 'best practice' set of processes for the secure and effective use of ContactPoint. The ContactPoint BPP bring together the Regulations, guidance and technical functions of ContactPoint and inform the development of ContactPoint Training and related materials.

The Best Practice Processes are made up of four separate but interrelated parts; these are:

- BPP1: Manage Data - outlines the processes which LA ContactPoint Management Teams should follow to meet the duties placed on them to manage data in ContactPoint.
- BPP2: Manage Users - outlines the processes which LAs and national partners should follow to manage users' access to ContactPoint. These include processes around detecting and investigating suspected misuse.
- BPP3: Manage Partners - outlines processes which LAs, national and local partner organisations should follow to ensure all organisations comply with the accreditation and audit requirements of ContactPoint.
- BPP4: Practitioners and Mediators - outlines the processes to be followed when practitioners access ContactPoint to search for a child and find out who is working with the same child.

C.03 **Best View** - where data from multiple sources is assembled by ContactPoint to form a single child record based on quality and reliability, and allows for alternative, multiple names and addresses to be displayed.

C.04 **Common Assessment Framework (CAF)** - The CAF for children and young people is a standardised approach to conducting an assessment of a child's additional needs at an early stage. CAF is a key part of delivering frontline services that are integrated and focused around the needs of children and young people.

The electronic enablement of CAF (**eCAF**) will be a single, national IT system to support the Common Assessment Framework. It will allow practitioners from different sectors to electronically create, store, and share a common assessment securely.

- C.05 **Consent** is agreement freely given to an action based on knowledge and understanding of what is involved and its likely consequences. Where consent is required for ContactPoint (to record contact details for sensitive services' practitioners, extending the retention of records beyond 18 or making a Subject Access Request) it must always be informed and explicit. **Informed consent** means that the person giving consent should understand what will be recorded on ContactPoint, who will be able to see this information and what might happen as a result of including or not including this information on ContactPoint. **Explicit consent** can be given orally or in writing, it must make direct reference to agreement to the actions/activity for which the consent is being sought.
- C.06 **Data** is defined under the DPA as meaning means information which is being processed by means of equipment operating automatically in response to instructions given for that purpose; is recorded with the intention that it should be processed by means of such equipment; and/or is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; it is an accessible record as defined in the DPA; or is none of the above but is recorded information held by a public authority.
- C.07 **Data cleansing** is the ongoing task of correcting or removing duplicate, inaccurate or mismatched data on ContactPoint.
- C.08 **Data Controller** - a person who either alone or with others determines the purposes for which, and the manner in which, any personal data are, or are to be, processed
- C.09 **Data Quality** - Data held on ContactPoint must be of a sufficiently high quality. Six key dimensions of this are:
- **Accuracy** - is the data correct? (e.g does the child live at this address, is this the correct birth date?);
  - **Recency/Currency** - how up-to-date is this data?;
  - **Coverage** – the number of children covered as a proportion of the total child population in England;
  - **Completeness** – the degree to which the full set of data required by ContactPoint is provided;
  - **Uniqueness** – the absence of duplicate child records within a data source; and,
  - **Validity** – the degree to which data provided complies with formatting requirements.
- C.10 **Data matching** is the comparison of data from more than one source in order to establish similarities and disparities relating to the same child. This is done, as far as possible, automatically by ContactPoint.

- C.11 **Data Subject** - is defined under the DPA as an individual who is the subject of personal data.
- C.12 **Enhanced Criminal records Bureau Disclosure (enhanced CRB)** - are required for posts that involve a far greater degree of contact with children or vulnerable adults. In general the type of work will involve regularly caring for, supervising, training or being in sole charge of such people. This disclosure involves an additional level of checking to those carried out for the Standard CRB - a check on local police records. Where local police records contain additional information that may be relevant to the post the applicant is being considered for, the Chief Officer of police may release information for inclusion in an Enhanced disclosure.
- C.13 **Lead professional** - a practitioner who takes the lead to co-ordinate provision and is a single point of contact for a child and their family, when a range of service providers are involved with that child or family and an integrated response is required (see *The Lead Professional: Practitioner's Guide*)
- C.14 **Learning difficulties** – Under section 13 of the Learning and Skills Act (2000) an individual has learning difficulties if (a) they have a significantly greater difficulty in learning than the majority of their peers or (b) they have a disability which prevents or hinders them from making use of facilities generally provided by post-16 education or training institutions. However, a person is not to be taken to have a learning difficulty solely because the language (or form of language) in which they are or will be taught is different from that which has been spoken in their home at any time.
- C.15 **'Local authority'** - means a children's services authority in England within the meaning of section 65(1) of the Children Act 2004:  
(a) a county council in England;  
(b) a metropolitan district council;  
(c) a non-metropolitan district council for an area for which there is no county council;  
(d) a London borough council;  
(e) the Common Council of the City of London;  
(f) the Council of the Isles of Scilly;
- C.16 **Local Safeguarding Children's Boards** - Local safeguarding children boards (LSCBs) are designed to help ensure that key agencies work effectively together to safeguard children, and put the former area child protection committees (ACPCs) on a statutory footing. LSCB membership includes local authorities, health bodies, the police and others (see Children Act 2004, s.13-16).
- C.17 **Mediated access** is where an authorised ContactPoint user accesses ContactPoint on behalf of another authorised user. Access rights are limited to the lowest common rights held by both the mediator and the 'mediatee'.

- C.18 **Metadata** –data which accompanies all data provided to ContactPoint. It includes the identity of the data source the time and date that data was provided to ContactPoint and useful data quality measures. Further metadata can be generated to assist in data matching and to create the audit trail of usage. Metadata is not displayed in the web interface or through adapted CMS.
- C.19 **National Partners** - those organisations listed in Schedule 2 of the Regulations, being organisations who may permit access to ContactPoint, are national charities, the Child Exploitation and Online Protection Centre (CEOP), and the Child and Families Court Advisory and Support Service (CAFCASS).
- C.20 **Ordinarily Resident** – Although there is no general statutory definition of ‘ordinary residence’, for the purposes of ContactPoint a child’s ordinary residence is usually determined by reference to their parents’ ordinary residence. For children who are subject to care orders (looked after children) the council with social services responsibility (CSSR) is responsible for that child’s record.
- C.21 **‘Participating Young Person’** - In the ContactPoint Regulations, a young person who has consented to information that is not archived information being held on ContactPoint, and who has not withdrawn that consent, is referred to as a “participating young person”. A participating young person is also a person subject to arrangements under section 10 of the Children Act 2004.
- C.22 **Partner organisations** are the key statutory and non-statutory agencies providing services for and coming into contact with children and young people, and are set out in the Children Act 2004 Information Database (England) Regulations 2007 (see B.02).
- C.23 **Personal data** is information about any identified or identifiable living individual and includes their name, address and telephone number as well as any reports or records.
- C.24 **Reasonable Steps** – All data controllers must carry out actions to ensure that information they are responsible for is and remains accurate. Local authorities can fulfil this duty with respect to ContactPoint data by notifying data sources where the data supplied does not match the ‘best view’ of a child record. Data sources must follow appropriate procedures for the data they hold.
- C.25 **Security Standards** - at the time of writing the relevant security standards covering the use of ContactPoint include:
- IS27001;
  - HMG Manual of Protective Security;
  - DCSF ContactPoint Security Statement;
  - DCSF Partner Workstation & Infrastructure Security (Jun 08);

- Detailed Integration Specification.

- C.26 **Security token** - an item or device which provides one of the elements of information required for authentication. Examples include a frequently changing numerical code generator or a single-use numerical (text) sent to your phone.
- C.27 **Serious Case Review** - Chapter 8 of *Working Together to Safeguard Children* (see C.39), sets out the purpose and process of serious case reviews (SCRs). SCRs are undertaken when a child dies (including suicide), and abuse or neglect is known or suspected to be a factor in the death. Additionally they can be undertaken where other serious concerns or safeguarding issues arise.
- C.28 **Serious Crime** for the purpose of this guidance, this means any crime which causes or is likely to cause significant harm to a child or serious harm to an adult.
- C.29 **Sensitive services** are a set of services where there is a strong public expectation and practitioner culture that information will only be shared where informed, explicit consent has been secured.

For the purposes of ContactPoint, sensitive services are defined as:

**Sexual Health** – Information, advice and treatment for pregnancy, abortion, contraception; sexually transmitted infections including services related to HIV/AIDS or Hepatitis B or C; rape crisis or sexual violence; sexual abuse and services related to Gay/Lesbian or Trans-Gender issues;

**Mental Health** – Child and Adolescent Mental Health Services tiers 2, 3 and 4 which includes referrals to, and assessment and treatment by, community based and in-patient teams dealing with, for example, sexual abuse and eating disorders; and

**Substance Abuse** – information, advice and treatment for drug, alcohol or volatile substance abuse (glue, aerosols and butane gas).

- C.30 **Significant harm** - there are no absolute criteria on which to rely when judging what constitutes significant harm. Consideration of the severity of ill-treatment may include the degree and the extent of physical harm, the duration and frequency of abuse and neglect, the extent of premeditation, and the presence or degree of threat, coercion, sadism, and bizarre or unusual elements. Each of these elements has been associated with more severe effects on the child, and/or relatively greater difficulty in helping the child overcome the adverse impact of the maltreatment. Sometimes, a single traumatic event may constitute significant harm, for example a violent assault, suffocation or poisoning. (see *Working Together to Safeguard Children* - see C.48).
- C.31 **Specialist and targeted services** - any service which is not normally provided to all persons in a particular age group. (Regulation 2(1), Interpretation.

- C.32 **'Staff'** - in this document, reference to the term 'staff' means a person employed, whether under a contract of service or a contract for services, seconded to the organisation, or working as a volunteer, for that organisation or LA.
- C.33 **Subject Access Request (SAR)** is a request made under the DPA by an individual to a data controller to see information which is held about them by the data controller.
- C.34 **Sufficient Understanding** - Children aged 12 or over may generally be expected to have 'sufficient understanding'. Younger children may also have sufficient understanding. The following criteria should be considered in assessing whether a particular child on a particular occasion has sufficient understanding to consent, or refuse consent, to sharing of information about them:
- Can the child understand the question being asked of them?
  - Does the child have a reasonable understanding of:
    - what information might be shared?
    - the reasons for sharing the information?
    - the implications of sharing or not sharing that information?
  - Can the child or young person:
    - appreciate and consider the options open to them?
    - weigh up one aspect of the situation against another?
    - express a clear personal view - distinct from repeating what someone else thinks they should do?
    - be reasonably consistent in their view on the matter - or are they constantly changing their mind?
- C.35 **Well-being** has a definition based on the five *Every Child Matters* outcomes. The achievement of these outcomes is in part dependent upon effective work to safeguard and promote the welfare of children.

## **ContactPoint Reference**

### C.36 **Information to be included on ContactPoint**

The **basic demographic details** that are held on a child's record are:

- name;
- address;
- gender;
- date of birth;
- a unique identifying number; and,
- where the child has died, the date of death.

The **contact details** for the parent or carer for the child or young person.

Contact details are held for the people or bodies which provide universal services to the child. These are educational setting, GP practice and, where applicable, midwife, health visitor and school nurse.

Contact details are also recorded for practitioners and services working with

that child providing a range of additional (specialist/targeted) services.

Contact details for those providing sensitive services (see C.29) can be indicated as an unspecified sensitive service involved. Sensitive services may only be indicated: a) with the consent of the child or young person; or b) if the person or body providing the service considers there is reasonable cause to suspect that the child or young person is suffering or is likely to suffer significant harm. The details of this service will not be visible to users, and contact will only be possible where the practitioner providing the sensitive service deems it appropriate.

**CAF, lead professional and other information** - ContactPoint indicates whether an assessment using the CAF has been undertaken for a child and provides contact details for the practitioner who holds that assessment information.

Metadata relating to information specified above.

ContactPoint does **not** hold case records held by different organisations, and it does not record statements of a child's needs, academic performance, attendance or clinical observations about a child.

ContactPoint is populated from a number of national and local data sources, including case management systems. This is a one-way process - ContactPoint does not allow users to access case management systems, the information held on them, or records held by children's services agencies.

**C.37 Persons and bodies required to disclose information to ContactPoint (see regulation 11 and Schedule 4 of the ContactPoint Regulations) - [http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1)):**

- a children's services authority in England;
- a district council which is not such an authority;
- a Strategic Health Authority;
- a Special Health Authority, so far as exercising functions in relation to England, designated by order made by the Secretary of State for the purposes of this section;
- a Primary Care Trust;
- an NHS trust all or most of whose hospitals, establishments and facilities are situated in England;
- an NHS foundation trust;
- the police authority and chief officer of police for a police area in England;
- the British Transport Police Authority, so far as exercising functions in relation to England;
- a local probation board for an area in England;
- the Secretary of State in relation to his functions under sections 2 and 3 of the Offender Management Act 2007, so far as they are exercisable in relation to England;
- a youth offending team for an area in England;
- the governor of a prison or secure training centre in England (or, in the

- case of a contracted out prison or secure training centre, its director);
- any person to the extent that he is providing services under section 114 of the Learning and Skills Act 2000 (c. 21).
- the Learning and Skills Council for England;
- the governing bodies of maintained schools in England (within the meaning of section 175 of the Education Act 2002)
- the governing bodies of institutions in England within the further education sector (within the meaning of section 175 of the Education Act 2002)
- the proprietors of independent schools in England (within the meaning of the Education Act 1996)
- the governing bodies of special schools which are not maintained by a local authority and which have been approved as a special school under section 342 of the Education Act 1996
- the Registrar General for England and Wales
- any other person or body specified by the Secretary of State in regulations.

**C.38 Persons and bodies permitted to disclose information to ContactPoint** (see regulation 11 and Schedule 5 of the ContactPoint Regulations) -

- a person registered in England for child minding or the provision of day care under Part 10A of the Children Act 1989 (c. 41);
- a voluntary organisation which holds information on children in the area;
- the Commissioners of Inland Revenue;
- a registered social landlord;
- healthcare professionals (regulated by a body specified in Section 25(3) of the NHS Reform and Health Care Professions Act 2002);
- the fire and rescue authority for any area in England where the LA is not the fire and rescue authority for the area; and,
- Children and Family Court Advisory and Support Service (CAFCASS).

**C.39 Persons authorised to use ContactPoint** (see Regulations, Schedule 3) - Access to ContactPoint (both direct and mediated) will be granted according to the role of the practitioner. The ContactPoint regulations set out the types of practitioner who may be authorised to access the ContactPoint. These are:

- Anyone employed by, or contracted to provide services to, a LA, who carries out functions under sections 10 and 11 of the Children Act 2004;
- LA social services staff (including children's home, residential family centre and foster care staff);
- LA Children's Trust staff;
- Staff responsible for carrying out Local Education Authority functions under parts IV and parts VI of the Education Act 1996 and section 175 of the Education Act 2002 (Duties in relation to the welfare of children);
- Regulated health care professionals (and administrative/support staff);
- Police officers, community support officers, special constables, the British Transport Police and police authority staff;
- Local probation board officers;
- Members of a youth offending team;

- Staff of a prison, youth offending institute or secure training centre (including those which are contracted out);
- LA staff providing advisory services on education and training to 13-19 year olds (currently provided by Connexions);
- Staff in a maintained school (including head teachers, deputy head teachers, heads of year, teachers with pastoral responsibilities, SEN teachers; SENCOs and equivalents);
- Staff in an FE college (includes principals, senior managers, and those involved in learner support including SENCOs);
- Staff in an independent school or non-maintained special school (with equivalent roles to those listed for the maintained sector);
- Staff of a voluntary and community sector organisation;
- Service managers and family court advisors in Children And Families Courts Advisory and Support Services (CAFCASS);
- Fire and Rescue authority staff involved in education and participation programs; and
- Staff of the Child Exploitation and Online Protection (CEOP) centre.

## Further Sources of Reference

### C.38 DCSF

**Acceptable Use & Privacy Policy** (available on LARA)

### C.39 **Adoption and Children Act 2002** and supporting legislation:

<http://www.everychildmatters.gov.uk/socialcare/childrenincare/adoption/act2002/legislation/>

### C.40 **Statutory guidance materials** produced under the **Children Act 2004** for agencies covered by the duty to co-operate to improve wellbeing and by the duty to safeguard children and promote their welfare (Sections 10 and 11):

<http://www.everychildmatters.gov.uk/strategy/guidance/>;

Further information on ContactPoint is available on the **ECM website**:

<http://www.ecm.gov.uk/contactpoint/>

### C.41 Guidance on the **Common Assessment Framework** for children and young people (CAF):

<http://www.everychildmatters.gov.uk/delivering services/caf/>

### C.42 **Detailed Integration Specification (DIS) v.2.0** (available on LARA)

### C.43 **Every Child Matters Green Paper**:

<http://www.everychildmatters.gov.uk/publications/>

Every Child Matters was published in September 2003 alongside a detailed response to Lord Laming's Report into the death of Victoria Climbié, and sought views from vital groups of staff and professionals committed to meeting children's needs.

- C.44 Cross-government **Information sharing: Practitioners guide**, *Information sharing: Case examples* and *Information sharing: Further guidance on legal issues*:

<http://www.everychildmatters.gov.uk/deliveringservices/informationsharing/>

Case examples, training materials and further information about powers/legislation: [www.everychildmatters.gov.uk/](http://www.everychildmatters.gov.uk/)

- C.45 Guidance on **Lead Professional**:  
<http://www.everychildmatters.gov.uk/deliveringservices/leadprofessional/>

- C.46 **Local Authority Readiness Assessment Tool (LARA)**:

- C.47 **Security Statement**:  
[www.ecm.gov.uk/contactpoint](http://www.ecm.gov.uk/contactpoint)

- C.48 **Working Together to Safeguard Children** (DfES, 2006) statutory guidance which sets out what to do to safeguard and promote the welfare of children: [www.everychildmatters.gov.uk/socialcare/safeguarding/](http://www.everychildmatters.gov.uk/socialcare/safeguarding/)

- C.49 **Information Commissioner's Office**

The **Data Protection Act 1998**:

[http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

**Subject Access Request**: [www.ico.gov.uk/](http://www.ico.gov.uk/)

- C.50 **Cabinet Office**

Privacy and data-sharing: the way forward:

[http://www.cabinetoffice.gov.uk/strategy/work\\_areas/privacy.aspx](http://www.cabinetoffice.gov.uk/strategy/work_areas/privacy.aspx)

- C.51 **Department of Health**

*Confidentiality: NHS Code of Practice* (DH, 2003):

[www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf](http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf)

- C.52 **General Medical Council**

0-18 years: guidance for all doctors (2007): [http://www.gmc-uk.org/guidance/ethical\\_guidance/children\\_guidance/index.asp](http://www.gmc-uk.org/guidance/ethical_guidance/children_guidance/index.asp)

- C.53 **Nursing and Midwifery Council**

*The NMC Code of Professional Conduct: Standards for Conduct, Performance and Ethics* (NMC, 2004):

[www.nmc-uk.org/aFramedisplay.aspx?documentID=201](http://www.nmc-uk.org/aFramedisplay.aspx?documentID=201)

**C.54 Youth Justice Board and the Association of Chief Police Officers**

*Sharing Personal and Sensitive Personal Information on Children and Young People at Risk of Offending: A Practical Guide* (YJB, 2005):

[www.youth-justice-board.gov.uk/Publications/Scripts/prodView.asp?idproduct=211&eP=PP](http://www.youth-justice-board.gov.uk/Publications/Scripts/prodView.asp?idproduct=211&eP=PP)