Draft ContactPoint Guidance

Version 1

1 INTRODUCTION

1.1 Purpose of this guidance

This document is guidance issued under section 12(12) of the Children Act 2004. It sets out the key statutory requirements of section 12 and regulations made under it, and provides support to ensure the appropriate use and operation of ContactPoint.

1.2 Regulations (the Children Act 2004 Information Database (England) Regulations 2007) place particular duties on local authorities to:

- participate in the operation of ContactPoint;
- supply relevant data held on local authority systems about children for inclusion on ContactPoint;
- ensure the completeness and accuracy of the records for children ordinarily resident in their area; and
- establish and maintain a complaints procedure in relation to the operation of ContactPoint in their area.

1.3 Section 12 requires that any person or body establishing or operating a database under section 12 of the Children Act 2004 must (in the establishment or operation of the database) have regard to any guidance given to them by the Secretary of State. This means that local authorities and any national partners which ContactPoint Regulations specify may manage their own users, must follow this guidance and, if they decide to depart from it, must have clear and justifiable reasons for doing so.

1.4 In addition, this guidance is for all those who will have access to ContactPoint (ContactPoint users) and their managers (staff managers), bodies which supply data, and partner organisations which can also establish and manage user accounts for their own employees. For a list of these bodies and individuals, see *Glossary.*

1.5 All ContactPoint users must comply with all relevant provisions in legislation. This includes the Children Act 2004 Information Database (England) Regulations 2007; the Computer Misuse Act 1990 and the Data Protection Act 1998 (see A1 & A10-A11).

1.6 Purpose of ContactPoint

ContactPoint is established under section 12 of the Children Act 2004 and is part of the Every Child Matters: Change for Children Programme. The purpose of ContactPoint is to support practitioners, local authorities and other organisations in fulfilling their duties under section 10 (duty to cooperate to improve well-being), 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 local authority duties established by section 4 of the Education and Inspection Act

2006 to identify children not receiving education. (see A5-A6)

1.7 ContactPoint is an electronic tool which supports practitioners in their work with children. It helps users to verify the identity of a child and to get contact details for other practitioners working with the same child. They can then make contact with them more quickly and easily, enabling them to work together more effectively.

1.8 ContactPoint design

The design of ContactPoint will comprise of a centrally maintained national system with a record for each child[1] (child record). Each local authority will be assigned responsibility for child records of children understood to be ordinarily resident in the authority. For looked after children, the Council with Social Services Responsibility will be responsible for the child record. ContactPoint will automatically assign records to a local authority based on available data. If the ordinary residence of a child is known to differ from this automatic assignment, the local authority to which the record was assigned must identify the local authority that should be responsible for the record and agree a transfer.

1.9 Accuracy

For ContactPoint to be a useful tool for practitioners working with children the information it holds must be accurate and up to date. All those who manually update data on ContactPoint, or enter data into systems which supply data to ContactPoint, must fulfil their duties under the Data Protection Act 1998.

1.10 Security

Keeping the information on ContactPoint safe and secure and ensuring that it is only accessed by people who have a right to access it is of paramount importance, this too is a requirement of the Data Protection Act. Everyone who uses, administers and manages ContactPoint must act in ways that preserve the security of ContactPoint.

1.11 How to read this guidance

The sections of this guidance in chapters 2, 3 and 4 are structured around principles and processes. For each section, there will be general guidance for all readers, and guidance targeted at specific groups. This targeted guidance is presented in colour-coded and labelled boxes. This is intended to assist you in quickly identifying the guidance that is relevant to your role.

1.12 You role may move between or cover more than one of these groups simultaneously. You should read all sections relevant to your involvement with ContactPoint. These groups are outlined in the following table -

[1] The terms ‘child’ and ‘children’ used throughout this document to refer to infants, children and young people aged 0 to 18

1.13

User Groups	Roles of users	Description
CONTACTPOINT USER	Practitioner or equivalent	Individuals authorised to use ContactPoint to support their work with children
	Manager/ supervisor	Practice managers and team leaders authorised to use ContactPoint and manage other practitioners working with children
	Practitioner Support staff	Other staff authorised to use ContactPoint to support practitioners and managers in their functions (e.g. school administrator)
STAFF MANAGER	Staff manager of any ContactPoint user	A non-ContactPoint user responsible for supervising or line managing practitioners or support staff who are authorised ContactPoint users
CONTACTPOINT MANAGEMENT TEAM	LA ContactPoint manager	Responsible for the operation of an LA compartment of ContactPoint includes handling complaints and subject access requests
	LA data administrator	Responsible for maintaining data quality of records for which LA is accountable (assigned to them)
	user account administrator	Responsible for establishing and administering ContactPoint user accounts – In a LA or national partner

1.14 A further group referred to in this guidance but not identified above is the central (national) ContactPoint team, responsible for operating the central ContactPoint system (managing national data sources, national reporting, central governance and system maintenance). This guidance is not intended for the central ContactPoint team.

1.15 Force of this guidance

[The statutory elements of this guidance came into force on xx XXX 2007, and apply to England only.]

1.16 Other materials

In places throughout this guidance, reference is made to further operational guidance, training and other materials, issued to support fully the use and operation of ContactPoint. These materials should be read and used in conjunction with this guidance.

2 ContactPoint ACCESS

This chapter covers obtaining authorisation to access ContactPoint information, methods of access and security. The topics covered are:

- Security principles (2.1)
- Becoming a ContactPoint user (2.7)
- Accessing ContactPoint (2.12)

2.1 Security principles

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

2.2 To ensure that only legitimate users access ContactPoint, a password and a physical security token (see *Glossary*), are both required to authenticate identity. This is known as 2 factor authentication.

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

- Adhere to any local organisation policy/guidance on IT security;
- Never share user accounts, passwords or security tokens with others;
- Do not write down your password and take care when entering it to ensure your keyboard is not overlooked;
- Keep 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 within a public environment; and
- Do not use public terminals (e.g. internet cafes, public reception areas) to access ContactPoint.

2.4 Users

It is your responsibility to prevent others from gaining access to, or making use of, your account. You must not share your password or security token with others. If you intentionally facilitate unauthorised access to ContactPoint, it is likely you are committing an offence under the Computer Misuse Act 1990 (see A10). You are likely to be committing an offence under this act if you make unauthorised or inappropriate use of ContactPoint yourself.

You must keep your password secret and look after your security token. Failure to do so may result in suspension or closure of your ContactPoint account. You may also be subject to your organisation's disciplinary procedures. If you forget your password or cannot gain access to the system, contact your user account administrator - they will reset your password if appropriate.

If you think your password may be known to others, or you have lost your

security token then you must inform your user account administrator **immediately** to enable them to take appropriate action. Any access using your password or security token, will register in the audit trail as activity carried out by you.

2.5 Staff Managers

You should ensure that all users you manage are aware of the importance of security, understand good security practice and act in a way which will not compromise ContactPoint. If you suspect a staff member is breaching security, you should contact the **ContactPoint Management Team** to discuss necessary steps, which may include disciplinary action.

2.6 ContactPoint Management Team

LA and **partner organisation user account administrators** - You are responsible for administering user accounts and the security arrangement related to user accounts. User accounts and security tokens must only be issued to individuals who meet ContactPoint access requirements (See 2.7).

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. You can only reactivate a user account after the user has been provided with a new, secure password and/or token as required.

2.7 Becoming a ContactPoint user

Access to ContactPoint is restricted to those who are permitted by Regulations, and who fulfil all of the conditions in regulations. Most applicants will meet some of these conditions already. Users must:

- need access for part or all of their work;
- have completed accredited ContactPoint training;
- have undertaken any other training which the local authority (or national partner) considers appropriate;
- have an enhanced CRB disclosure which is less than 3 years old; and
- be a member of the Vetting and Barring Scheme[2] (once operational and ContactPoint Management Teams have been advised that this requirement is active) (see *Glossary*).

2.8 ContactPoint training will cover how a practitioner accesses ContactPoint, and explain the responsibilities of all authorised users regarding data accuracy, searching and updating child records. Training will also cover the importance of security and good security practice and all relevant legislation including the Data Protection Act and the Human Rights Act.

2.9 The requirement to have an enhanced CRB disclosure which is renewed every three years is specific to ContactPoint and does not replace existing

[2] Established by the Safeguarding Vulnerable Groups Act 2006 and due to come into operation in Autumn 2008

organisational policies for non-ContactPoint users. Individuals who do not have an enhanced CRB disclosure or have one which is more than 3 years old will have to apply for a new disclosure to become ContactPoint user. Applications for enhanced CRB disclosures should be made in sufficient time to receive it before access is needed (or a previous disclosure reaches 3 years). If evidence of a renewal is not received before the 3 year period the user account may be suspended.

2.10 **Users**

If you are applying to become a user and wish to use your existing enhanced CRB disclosure you will need to demonstrate that this disclosure supports your suitability to access ContactPoint. Your employer may be asked for written confirmation of your suitability. You may be asked to show your disclosure to the ContactPoint management team. You do not have to do this, but if the ContactPoint management team cannot confirm the suitability of an existing disclosure, either directly or through your employer you will have to apply for a new enhanced CRB disclosure.

2.11 **Staff Managers**

You should assist the staff you manage in fulfilling the access requirements for ContactPoint. This will involve releasing them to attend ContactPoint training, and where necessary supporting them in applications for a new or renewed enhanced CRB disclosure.

If an applicant is planning to use an existing CRB disclosure to fulfil the access requirements for ContactPoint you may be contacted by the ContactPoint management team. You will be asked to confirm in writing the disclosure has been obtained in the last 3 years for the individual's present role. You must also confirm that, based on this disclosure, you judge the individual to be suitable to access ContactPoint (see 4.30).

An enhanced disclosure is tailored to the position for which it was obtained. Using a previously obtained disclosure is described as 'portability'. The CRB website (www.crb.gov.uk) provides information to help you decide if it is appropriate for you to confirm the disclosure is sufficient. If you are uncertain, a new enhanced disclosure should be sought for the applicant to become a ContactPoint user.

2.12 **Accessing ContactPoint**

Authorised users can access ContactPoint by three routes: web interface; adapted case management system; and mediated access. Each is subject to the same high level of security.

2.13 **Direct Access** (see flowchart B6)

- **Web interface -** This is where users login using their user account, password and security token through a website to access ContactPoint. Users can use the web interface to search for, manually

update or create new child records.

- **Adapted Case Management System -** This is where a Case Management System (CMS) has been adapted to allow direct access within an existing user system. Authorised users will be able to access ContactPoint functionality through their own organisation's CMS. Any adapted CMS will be fully accredited to ensure it meets the necessary security standards.

2.14 **Users**

Direct access will usually occur in a wide variety of office or working environments. You are expected to take precautions to ensure that the workspace in which you access ContactPoint does not compromise security (see 2.1-2.6).

2.15 Mediated access

Mediated access is where one authorised user accesses ContactPoint via another authorised user. Any ContactPoint user who has been granted the appropriate access rights can act as a mediator, but only for another authorised ContactPoint user. Where access is mediated, the details of both requestor and mediator will be recorded in the audit trail.

Mediated access is different to brokered access for sensitive service information (see 3.48-3.52).

2.16 **Users**

Requestor - To request mediated access to ContactPoint you should contact another authorised user to mediate your access, and provide authentication information to confirm that you are an authorised user.

Mediator - To ensure that the individual making the request is an authorised user you will be required to enter their authentication information before you can mediate their access.

You must not allow access on behalf of colleagues who are not authorised users to access ContactPoint or provide mediated access without carrying out the required authentication procedures. This is considered inappropriate use. Only your user details would be recorded in the audit trail.

2.17 **ContactPoint Management Team**

Mediators – you must follow the guidance provided above. Users who do not have direct access to ContactPoint should be aware of what mediated access arrangements have been established in your local area.

3. USING ContactPoint

This chapter contains guidance on using ContactPoint. This falls into two broad sections; the first deals with aspects relating to working with ContactPoint; the second sets out how ContactPoint can support practitioners in their broader duties and activities.

Working with ContactPoint:

- Ensuring accuracy (3.1)
- Consent (3.3)
- Misuse of ContactPoint (3.9)
- Searching for and identifying a child record (3.13)
- Creating a new child record (3.19)
- Amending/updating a child record (3.23)
- Recording involvement (3.26)
- Sensitive services, CAF and lead professional (3.30)
- Setting the age for archive above 18 (3.34)
- Recording date of death (3.37)
- Indicating an involvement has ceased (3.41)

Using ContactPoint to Support Practice:

- Communication with other practitioners (3.45)
- Brokering contact with sensitive services (3.48)
- Engaging children and parents/carers (3.53)
- Ensuring continuity of service provision (3.58)
- Children not receiving education (3.62)
- Case reviews and enquiries (3.65)

3.1 Ensuring accuracy

Everyone who processes data about individuals is bound by the 4th Principle of the Data Protection Act (See A11), to ensure all records are accurate and up to date. ContactPoint creates child records by matching information from different data sources and generating a 'best view' based on this information (*see Glossary*). Where data items from a data source do not match this 'best view' an automatic notification is sent to the data source to highlight that data which may be inaccurate or out-of-date. This supports the requirement for local authorities to take reasonable steps to notify data sources, where information appears to be inaccurate. Data sources cannot be provided with the information that is held in the 'best view', they must follow their own procedures for investigating possible inaccuracies.

3.2 Users

You play a key role in ensuring that ContactPoint is accurate. You should take all reasonable steps to keep your own Case Management System (CMS) records accurate and up to date. If your CMS automatically provides data to ContactPoint, any inaccurate data will be passed to ContactPoint.

You should not assume that records on your own CMS or on ContactPoint are correct and up-to-date. Where you identify a discrepancy between systems you should take action to verify the correct information, this should usually be done by checking with the child and their parent/carer. You should then update your CMS or ContactPoint as appropriate.

If your CMS automatically updates ContactPoint you do not need to update ContactPoint directly, your CMS which will feed updates to ContactPoint. If your CMS does not provide data to ContactPoint, you should manually update a child record using the web interface or through mediated access.

3.3 Consent

Consent is only required to hold a child record on ContactPoint past the age of 18 years old (see 3.34-3.36), or to indicate involvement of a 'sensitive service' on a child record (see 3.30-3.33).

3.4 In these two circumstances, informed and explicit consent (see C2) must always be sought. It must be sought from the child where they are judged to have sufficient understanding to give or withhold their consent. Where the child does not have sufficient understanding, consent should be sought from their parent/carer.

3.5 Consent relating to ContactPoint can be sought as part of a broader request for consent. 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.

3.6 Organisations will already have procedures relating to consent for their own records, and to broader information sharing practice. Detailed guidance on consent and competency is available in the *Information Sharing: Practitioner's Guide - paragraphs 4.12-4.22* (see C25).

3.7 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. When consent is withdrawn the practitioner or service should inform the ContactPoint management team who will move the involvement straight to archive.

3.8 Recording involvement without consent

Sensitive service involvement can be recorded or retained on ContactPoint without consent where there is an overriding public interest in doing so. The situations where it is appropriate to record involvement without consent are rare and consent should always be sought, unless seeking consent would put a child or adult at risk of significant harm. Involvement should only be recorded without consent where the person or body supplying the data considers that there is reasonable cause to suspect that the child is suffering,

or is likely to suffer significant harm.

3.9 **Misuse of ContactPoint**

Using ContactPoint for other purposes than to support practitioners in fulfilling specific duties (see 1.6) or in a manner contrary to this guidance is likely to be misuse (see flowchart at B13). For instance, it would not be appropriate for ContactPoint to be used to assess applications for school places, or to pinpoint an adult suspected of tax-evasion. Nor is it appropriate for ContactPoint users to access records of their own children, or those of their colleagues, friends and neighbours, unless they have a legitimate professional relationship as a provider of services to that child.

3.10 **Users**

When you access ContactPoint your reason for doing so will be recorded in the audit trail. You should be prepared to explain your activity, when asked, by your staff manager or members of the LA ContactPoint Management Team. Circumstances where your use might be considered unusual include:

- Higher than average activity for your role/profession;
- Frequent searches outside your local authority area;
- Searching for records of family members;
- Out-of-hours usage; or,
- Broad-criteria or repeat-criteria searches.

3.11 **Staff Managers**

You should ensure that those you manage fully understand the implications of misusing ContactPoint.

You should support ContactPoint Managers where they are carrying out enquiries and investigations into potential misuse. You should record all actions and decisions and be ready to apply your organisation's disciplinary procedure where this is necessary.

3.12 **ContactPoint Management Team**

LA and Partner organisation user account administrators - It is your responsibility to monitor the activity of users in your area or organisation, to detect misuse. Where unusual use has been identified, you should investigate immediately, suspend the account if necessary (see 4.34-4.39) and notify their staff manager. The user should be asked for an explanation of their activity. Care should be taken not to regard all apparent misuse as wilful. For example it may be due to a training issue. It may be more appropriate for the user's manager to seek this information in the first instance. You should record any reason given by the user, the outcome of your enquiry, and any decision made regarding the user's access.

If further investigation is necessary, the following responsibilities apply:

- where a user is authorised by a national partner, this investigation

should be carried out within that organisation; or
- where a user is authorised by a local authority the LA ContactPoint Manager should carry out this investigation. This applies to staff of the local authority and partner organisations. The ContactPoint manager should work with the user's staff manager during an investigation.

If this investigation proves satisfactory, you should reactivate the user's account and record all decisions made/action taken. If further investigation demonstrates that misuse has occurred a number of sanctions are available. The application of sanctions is dependent on the severity of the misuse identified, and includes:

- permanent deletion of the user account;
- disciplinary action within a user's organisation (this should be carried out by the user's manager);
- prosecution for offences under the Computer Misuse Act which can result in fines or imprisonment (see A10); and/or
- enforcement action by the Information Commissioner's Office for offences under the Data Protection Act 1998 (see A11-A14).

ContactPoint Managers – You must ensure that appropriate arrangements are in place to monitor all users in your area and identify misuse. This includes ensuring that arrangements are in place to regularly audit the access of all ContactPoint users.

3.13 **Searching for a child record**

A child record can be searched for using a range of details known about the child. Each time a search of ContactPoint is made, the user will record the reason for their search which is stored in the audit trail.

3.14 Where the search criteria entered return more than a limited number of matches, ContactPoint will not display the search results. Instead, the user will be asked for more details in order to complete the search.

3.15 ContactPoint records contain information from multiple data sources. These data sources may not always provide identical information (for instance they may hold different addresses). Users will see a 'best view' of a child record when accessed (See *Glossary*).

3.16 **Users**

Each time you carry out a search of ContactPoint you will need to select a reason for your search; this will be recorded in the audit trail. Even if you search ContactPoint using an adapted CMS or through mediated access you are subject to the same rules and guidance about your use.

3.17 **Staff Managers**

You should ensure that authorised users you manage understand that they may only search ContactPoint if they have an appropriate reason to do so.

3.18 **ContactPoint Management Team**

You need to be alert to any suspicious activity and make enquiries or investigate this immediately (see 3.9-3.12).

3.19 **Creating a new child record**

ContactPoint creates records automatically using basic demographic data about children from a number of national and local data sources. Not every child record will be complete.

3.20 ContactPoint will only hold records for children who are ordinarily resident in England (see *Glossary)*. A child record should not be created for a child who is resident outside of England but who accesses services in England.

3.21 **Users**

If you are the first practitioner to come into contact with a child, you should always search for an existing child record, using all of the information available to you. Before starting the process to create a new child record, you should make certain that there is no existing record for that child.

3.22 **ContactPoint Management Team**

Data administrators – Where a user has initiated the creation of a new child record, you should carry out further checks on the data the user submits to see if it can be matched to existing records. For authorities that are close to the borders or Wales and Scotland, it is possible that records may be created for children who are ordinarily resident outsider of England. Any records where a child's ordinary residence is outside England should immediately be removed from ContactPoint.

3.23 **Amending and updating a child record**

Information about a child may change at any time. When this happens, it is important that ContactPoint is updated either by amending Case Management System (CMS) records or by manually updating a ContactPoint child record through the web interface. Records must be updated to reflect changes to the details of the child, parent or carer, practitioner involvement, service provision, changes to practitioner details and when a service ceases.

3.24 **Users**

Where you believe that the information about a child has changed the ContactPoint child record may need to be updated. The most reliable way to check information is to ask the child or their parent/carer directly. Where a child or their parent/carer provides new information, it is good practice to verify this change. For instance, a new address could be verified by a domestic bill. You should update your CMS (if it automatically updates ContactPoint) or manually update ContactPoint as appropriate.

3.25 **ContactPoint Management Team**

ContactPoint data administrators – Some updates or amendments to records will be marked for your review. In cases where there is a conflict between the amendment and the existing child record which the system cannot resolve you should only manually override this where you have additional verification.

You are responsible for making changes to ContactPoint records where you have verification that this is necessary and for notifying data sources where the data they are providing may be inaccurate. You are not responsible for ensuring that a data source amends their records.

3.26 **Recording involvement**

ContactPoint records include the practitioners/services which are working with a child. These involvements divide into universal services which are provided to all children in an age range and specialist/targeted services which are only provided to some in an age group. Involvement is shown as an organisation, team or practitioner's contact details. Organisations providing specialist/targeted services should establish a policy to identify the areas of their activity which should be treated as involvements for the purpose of ContactPoint and therefore recorded on a child record.

3.27 Where the provision of a service is transferred to another team member, the child record must be updated to reflect this. The new practitioner then takes over responsibility for maintaining their data on the child record for the duration of their involvement. When an involvement finishes this is also recorded (see 3.41-3.44).

3.28 **Users**

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.

If your organisation is **required** to supply data to ContactPoint, you must ensure that your involvement is indicated on the records of all children you work with. If your organisation is **permitted** to supply data to ContactPoint, you should follow your organisational guidelines about when to record involvement. If you have provided data, whether you are permitted or required to supply it, ContactPoint regulations require you to keep information about your involvements accurate and up to date.

You may provide a specialist/targeted service within the context of a universal service (e.g. SEN provision in a school). Your involvement as a practitioner/service should be recorded on a child record in addition to the contact details of the universal service if this is in line with your organisation's policy on recording involvement.

Where your involvement is separately recorded on a child record, this

indicates to other users that you are taking some form of action with a child and that you may have important information to share. This information may be your own knowledge or more formal case records. Recording your involvement does not mean that you must share information – you should use your professional judgement to decide whether it is appropriate to share with any practitioners that contact you. Further guidance is available from the [Cross-Government] *Information sharing: Practitioners guide* (see C25).

3.29 **Staff Managers**

You should ensure that those you manage update their involvements as changes occur and regularly review this information on ContactPoint. It is particularly important that when an involvement is judged to have ceased this is marked on the child record (see paragraph 3.41-3.44). Where an involvement is not marked as ceased, practitioners may continue to make contact with those you manage – it is their responsibility to ensure the information is accurate and up-to-date.

3.30 **Sensitive services, CAF and lead professional**

In addition to universal and specialist/targeted services, ContactPoint can also show the following specific practitioner involvements:

- **Sensitive services** (See C17) - Where informed and explicit consent has been secured (See C2), sensitive services involvement will be indicated as an unspecified sensitive service. Contact details for this service will not be visible to users, and contact can only be brokered by the local ContactPoint management team (see 3.48-3.52).

- **Common Assessment Framework (CAF)** –This indicator shows the contact details for the practitioner or team that holds the most recent assessment undertaken using the CAF. These details will be held on the child record until a subsequent CAF assessment is undertaken. This information can be indicated by a user through secure web access or automatically provided by an e-CAF system;

- **lead professional** (See C9)– This is indicated on a child record where a lead professional is working with a child;

In some cases a CAF-holder or a lead professional may not be a ContactPoint user. Their contact details can still be recorded on a child's record by an authorised user, and contact can be made, but they will be unable to access ContactPoint themselves unless they apply to become a user. Practitioners who are performing these roles are likely to be eligible for access to ContactPoint and should usually become users to support their work.

3.31 **Users**

These indicators are not a substitute for taking necessary action or carrying out your duties to ensure the safety or wellbeing of a child.

Before undertaking an assessment using **CAF** you should always check ContactPoint to see if a CAF assessment has been undertaken. Where you are undertaking a common assessment for a child, you should indicate this on ContactPoint as soon possible. This will minimise the risk that another practitioner may start a separate CAF assessment for the child, duplicating your effort and frustrating the family.

If you are the **lead professional** for a child, this should be indicated on the child's record. This will allow other ContactPoint users to identify you and ensure that you are aware of all of the practitioners and services involved with a child.

You may be asked to record details of another practitioner's involvement if they are not an authorised ContactPoint user.

Sensitive service providers - When seeking consent (See 3.3-3.8) to add your contact details to a child record, you should:

- Judge whether a child is capable of giving consent themselves (they may still wish to involve their parent/carer);
- Explain the purpose of ContactPoint and that it only holds contact details, not any case information;
- Explain that details of the sensitive service will not be visible to other practitioner, contact can only be requested through 'brokering' by the ContactPoint Management Team;
- Explain that consent can be withdrawn at any point; and
- Confirm that this has been understood and that consent is given to record details on ContactPoint. You should record this agreement in your own records.

If consent is not given or is withdrawn, you must not place or retain your contact details on a child's record unless there is an overriding public interest in doing so (see 3.8). Where consent is withdrawn you should contact the ContactPoint manager so that they can amend the child record.

CAF-holder - If you work in a Sensitive Service and have undertaken a CAF assessment, you must obtain consent before you can indicate this on a child record. As far as possible, the nature of the service you provide will not be made visible on the record. If the child or family are not comfortable with your contact details being added as the CAF holder, it may be better for a practitioner who is not from a sensitive service (where there is one involved) to hold the CAF and add their contact details to ContactPoint.

Lead professional - If you are seeking consent to become the nominated lead professional and you provide a sensitive service you must ensure that the child or their family understand that in order for you to fulfil that role, your contact details as the lead professional must be displayed on ContactPoint. As far as possible, this will be in a form which hides the service or identity. If the child or family are not comfortable with your details being added to ContactPoint then another practitioner must act as lead professional.

3.32 **Staff Managers**

If your organisation provides a **sensitive servics**, you should ensure that all practitioners you manage are seeking informed and explicit consent before registering their involvement on a child's record (unless there is a risk of serious harm), recording on local records whether consent was granted, and that it is periodically renewed. Your own organisation's procedures should support this practice. You should ensure that those you manage explain clearly the implications of them taking the lead professional role or being the CAF holder and understand if they child or family are not comfortable with their details being visible to other users they should attempt to make alternate arrangements.

3.33 **ContactPoint Management Team**

LA ContactPoint manager - Where a non-ContactPoint user undertakes an assessment using the **CAF**, or is the **lead professional** for a child, you should input the name and contact details of the practitioner onto the relevant child record if this information is not automatically supplied by a data source.

If a **sensitive service** provider contacts you to inform you that consent has been withdrawn for their details to appear on a child record you must remove this information from the child record (by archiving it) as soon as possible unless there is an overriding public interest in doing so (see 3.8).

3.34 **Setting the age for archive above 18**

ContactPoint regulations allow for the retention of records for some young people up to the age of 25 where the young people give informed and explicit consent (see C2). This provision only applies to records of children in England who are leaving care and those with learning difficulties (see C5) who are receiving services under the Learning and Skills Act 2000. This is to support the transition to adult services, particularly where a young person has complex needs.

3.35 **Users**

You must seek the informed and explicit consent of the young person for their record to be retained after the age of 18. If you judge that the young person does not have sufficient understanding to make these decisions on their own, you should, where possible, involve their parents, carers, or a legal guardian if a court order has granted them responsibility, to assist the young person in making this decision.

If consent is withdrawn at any point you must contact the appropriate ContactPoint Management Team to have the child record removed to archive.

3.36 **ContactPoint Management Team**

ContactPoint Data Administrators – When consent to retain a record on

the archive above the age of 18 has been granted, the record may be retained up to their 25th birthday. You should confirm the retention with the practitioner annually. If the practitioner informs you that consent has been withdrawn you must move the record to archive (see 3.7).

3.37 **Recording date of death**

When a child dies, ContactPoint provides a means of minimising unnecessary or inappropriate contact with the family by practitioners, by recording a date of death. Any data source or user can notify ContactPoint of the death of a child. A child record will be moved to archive one year after the child's death, this will only be prompted when the Registrar General provides a confirmation of the death.

3.38 **Users**

Checking ContactPoint before making contact with a family can help ensure that you are fully aware of the situation, and act with appropriate sensitivity.

If you know that a child has died and this is not yet recorded on ContactPoint, you should update the child record if you are able to verify this, to ensure other users are aware. However, if your CMS automatically updates ContactPoint and holds this information, you should update your own system which will automatically update ContactPoint.

3.39 **Staff managers**

Your organisation should have policies in place for verifying and recording date of death. Your staff should be guided by these policies when providing information about child deaths to ContactPoint.

3.40 **ContactPoint Management Team**

Where notification of a death is received from any data source or user the child record will reflect this. Data provided by the Registrar General will confirm a death and initiate the archive of the child record

3.41 **Indicating an involvement has ceased**

When practitioner/service involvement ceases, contact details will remain on the child record for one year - this is the standard ContactPoint retention period. ContactPoint regulations state that this period may be extended beyond one year, up to a maximum of 5 years, by the practitioner/service where they judge that the information they hold about the child may be relevant to other users.

3.42 **Users**

When your involvement with a child ceases you must ensure that the date of this is recorded on ContactPoint. Similarly, if you discover that a child has left the area which your organisation provides services to, you should ensure that

ContactPoint is updated.

You can set the period of retention above the standard period of one year. You should do this when you believe that information you hold about a child may be important to other users for longer than a year. You should decide what length of retention (up to the 5 year maximum) is appropriate in the individual circumstances. You should review these retention decisions annually to ensure they remain appropriate.

3.43 **Staff Managers**

You should encourage individuals you manage to consider an appropriate retention period following the cessation of involvement, and not simply to extend the period to the maximum 5 years. This will vary depending on the circumstances of their involvement with a child.

3.44 **ContactPoint Management Team**

Where ContactPoint users extend the period of retention for more than the standard period of one year they should be asked to confirm that this is still appropriate on an annual basis. ContactPoint will prompt this confirmation.

Using ContactPoint to Support Practice

3.45 **Communication with other practitioners**

ContactPoint directly supports the duties of cooperation under sections 10 and 11 of the Children Act 2004, by providing a tool to allow practitioners to easily identify which other services are being provided to a child and contact details for the practitioners providing these services.

3.46 **Users**

The fact that your contact details are included on a child record is not a substitute for action, nor does it create a requirement for you to have to share information with other users. These decisions must be based on professional judgement, including whether you have, or should seek, consent to share, supported by organisational policies and procedures, information sharing training and *Information Sharing: Practitioner's Guide* (see C25).

If you decide to contact another ContactPoint user to discuss a child, you must as a minimum:

- identify yourself to the other user and in a way they can verify;
- confirm the identity of the other user;
- clearly identify the child who you are making contact about;
- explain clearly the reason for your enquiry; and/or
- explain what information you are requesting and your reason.

When you are contacted by another ContactPoint user, you must ensure that:

- you are confident of the identity of the person making the request (this

could be done by phoning back on a 'trusted' official phone number of that practitioner - e.g. a known office number);
- the child to be discussed is clearly identified and agreed; and
- it is clear if information you share will be passed on.

3.47 **Staff Managers**

You should encourage and support those you manage to use ContactPoint to identify and contact other practitioners where appropriate. You should make sure that you and those you manage understand your organisational policies on information sharing and that they have regard to the *Information Sharing: Practitioners' Guide* (see C25).

3.48 **Brokering contact with sensitive services**

Contact details for sensitive services will not appear in the 'best view' (see C1) of a child record. An indicator will show that an unspecified sensitive service is working with the child. The contact details of this service are only visible to appropriate members of the ContactPoint Management Team. This additional level of privacy is in place to ensure that children are not discouraged from accessing sensitive services.

3.49 The ContactPoint Management Team will 'broker' contact between a ContactPoint user and a sensitive service organisation or practitioner. They act only as an intermediary and will not judge whether contact is appropriate. The sensitive service makes the decision whether to make contact with the original practitioner themselves (see flowchart B11).

3.50 Brokering contact only applies to sensitive service and is not to be confused with 'shielding' records (see 4.63-4.69).

3.51 **Users**

If a child record indicates that an unspecified sensitive service is involved, and you wish to make contact with practitioners providing this service, you will need to contact your local ContactPoint Management Team. You will be asked for your details, the child's ContactPoint record number and the reason for seeking contact. The ContactPoint Management Team will 'broker' contact between you and the Sensitive Services practitioner, team or agency.

Requests to the ContactPoint Management Team for details on sensitive services should only be made where you judge this is necessary (e.g. where it may have a direct impact on your involvement or to convene a multi-agency panel).

Sensitive Services - If you are the sensitive service provider and the ContactPoint Management Team informs you of the request to make contact, you must consider the potential importance of the information you hold, whether or not you decide to make contact. If you decide not to, you must tell the ContactPoint Management Team as soon as possible, so that they can inform the requesting practitioner. You should record you decision locally and

be willing to justify, if necessary, your decision not to share.

3.52 **ContactPoint Management Team**

LA ContactPoint Managers – Users will contact you when they wish to make contact with a sensitive service which is working with a child. You should take their contact details and the reason for their request. You are not required to make a decision about this request, but should act only as a 'broker' by providing this information to the sensitive service contact for that child. They will decide whether it is appropriate to make contact. You must find out if the sensitive service does not plan to make contact so that you can inform the user who made the request.

3.53 **Engaging children and parents/carers**

It is important that children have an understanding of ContactPoint and how it may help them. Parents/carers should also be informed about ContactPoint and the kind of information which is held about a child. The Data Protection Act requires that all organisations which supply data to ContactPoint, inform children and parents/carers of this, through fair processing notices.

3.54 Local authorities must take steps to promote ContactPoint, and make materials available for children and parents/carers which explain ContactPoint, what basic information is held about a child and what rights they have to access this information and correct any errors (see 4.13). Nationally produced materials must provide the basis for any materials that are developed locally.

3.55 **Users**

You should explain ContactPoint to children and parents/carers. You may decide, where appropriate, to show them what you see when you access their record. Wherever possible you should confirm information on ContactPoint with a child or their parent/carer to ensure its accuracy. You must bear in mind that when a child reaches a sufficient level of maturity or understanding, they may not want to share their information with parents and carers.

3.56 **Staff Managers**

You should ensure that all ContactPoint users have access to materials explaining and promoting ContactPoint. These materials should be available from the ContactPoint Management Team in your local authority. You should also make these available, in public areas, wherever your organisation provides services to children.

3.57 **ContactPoint Management Team**

LA ContactPoint Managers – You must ensure that materials which explain the purpose and operation of ContactPoint, including materials specifically produced for children, parents and carers are available throughout your

authority. You should provide partner organisations with these materials as required. They should as a minimum explain:

- what information is held on ContactPoint;
- the purpose of ContactPoint (identifying relevant legislation);
- subject access requests and how one can be made (including sample wording to assist children in making a request); and
- how a complaint can be made (see 4.17-4.21).

Partner organisations - you should ensure that materials which explain ContactPoint to children and their parents/carers are available at the point of access for your services, and to users within your organisation. These will be available from the local authority ContactPoint management team.

3.58 **Ensuring continuity of service provision**

Families may not remember to inform all practitioners and organisations who provide services to a child that they are moving or have moved. ContactPoint can assist in supporting service continuity by enabling practitioners to locate contact details for a child and their parent/carer. It also enables practitioners coming into contact with them for the first time after they have moved, to identify and contact practitioners that were working with them in their previous location, to support the continuation of any service provision.

3.59 **Users**

Where you have been providing a service to a child who moves away from your organisation's area of responsibility, you must update the child record accordingly. This includes indicating that your involvement has ceased and if the child's address is now unknown to your service, or, where known, details of the new address.

If it is part of your role, you will also be able to use ContactPoint to identify children who appear to have stopped accessing services, for example children not receiving education (see 3.62-3.64).

3.60 **Staff Managers**

You should ensure that those you manage understand the importance of adding and updating their details on ContactPoint in order to support service continuity.

3.61 **ContactPoint Management Team**

LA ContactPoint managers - Where a child ceases involvement with all services in your local authority they may have moved to another area (see 4.53-4.62). However, you must retain responsibility for the child record until you are able to locate the child and agree with another local authority that the child record can be transferred.

3.62 **Children not receiving education**

There is a duty on local authorities to identify children not receiving education (Section 4 Education and Inspections Act 2006), to make arrangements to enable them to identify (so far as it is possible to do so), children of compulsory school age in their area who are not receiving a suitable education.

3.63 ContactPoint can help local authorities discharge this duty by recording the place where a child is being educated, where that is known. (See the *Statutory Guidance for local authorities in England to identify children not receiving education* which provides further guidance on these duties).

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

3.64 **Users**

Where no educational setting is recorded a child could be receiving an education in a setting other than at school or ContactPoint may not automatically receive information about the education that a child is receiving. It is also possible that 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 local authority.

If you work in the LA team responsible for identifying children not receiving education you may access a report which lists the records of all children known to ContactPoint in your area who do not have an educational setting recorded on their ContactPoint record.

3.65 **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.

3.66 To support statutory local safeguarding children boards (LSCBs)[3] 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 chronology of practitioner involvement.

3.67 **ContactPoint Management Team**

LA ContactPoint manager – Access to the archive, for the purpose of assisting a case review, can only be made by local authority ContactPoint Management Teams.

[3] Children Act 2004 Sections 13-16 and related regulations

4. ContactPoint ADMINISTRATION

This chapter provides guidance on the administrative and management functions relating to administration of ContactPoint. These include processes relating to user accounts and to data and records. The topics covered are:

- Governance (4.1)
- Ensuring data quality (4.6)
- Subject access requests (4.7)
- Complaints procedure (4.17)
- Reporting and management information (4.22)
- Partner organisations administering user accounts (4.25)
- Creating a new ContactPoint user account (4.29)
- Suspending a ContactPoint user account (4.34)
- Closing a ContactPoint user account (4.40)
- Audit of ContactPoint usage (4.43)
- Establish a local data feed (4.45)
- Data matching and data cleansing (4.51)
- Child moves between local authorities (4.53)
- Child leaves England (4.60)
- Shielding records (4.63)
- New identities (4.70)
- The archive (4.74)

4.1 Governance

Governance of ContactPoint relates to the appropriate 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.

4.2 The governance of ContactPoint is divided between the Department for Education and Skills, local authorities, and partner organisations (*see Glossary*). The Secretary of State for the Department for Education and Skills is responsible for national governance of ContactPoint. Within each local authority, the Director of Children's Services is responsible for local governance. Operationally, this will be carried out by the local authority ContactPoint Management Team.

4.3 The ContactPoint Regulations specify persons in certain national partner organisations who may manage users within their own organisation. These organisations have responsibility for the aspects of operation which relate to management of users.

4.4 Each local authority is responsible for:

- establishing a ContactPoint team with appropriate skills and experience to establish and operate the system at a local level;
- managing and ensuring the accuracy of data (as a data controller) in child records which are assigned to it;
- Establishing secure local data supply agreements and ongoing

relationships with local data suppliers;
- organising training for ContactPoint users;
- creating, suspending and closing local user accounts;
- managing local access to the archive;
- handling complaints which relate to ContactPoint;
- responding to subject access requests;
- monitoring, auditing and investigating use of ContactPoint by local users;
- producing local statistics to support service planning; and
- promoting ContactPoint.

4.5 Local authorities must establish a team with sufficient technical and practical expertise to handle the responsibilities outlined in this guidance and the operational management of ContactPoint at a local level. Further guidance on the roles and responsibilities of this team is available to local authorities.

4.6 **Ensuring data quality**

Data held on ContactPoint must be of a sufficiently high quality, four key dimensions of this are:

1) **Coverage** – the number of children covered as a proportion of the total child population in England;
2) **Completeness** – the degree to which the full set of data required by ContactPoint is provided;
3) **Uniqueness** – the absence of duplicate child records within a data source; and,
4) **Validity** – the degree to which data provided complies to formatting requirements.

All data controllers of systems that provide data to ContactPoint already have responsibilities under the Data Protection Act 1998 to ensure that data they hold about an individual is accurate and up-to-date.

4.7 **Subject access requests**

Individuals have the right to request access to any personal data which an organisation holds about them (Section 7 of the Data Protection Act 1998). This is known as a 'subject access request'. The organisation processing the personal data is known as the 'data controller' in respect of the information. In the case of information held in a ContactPoint record, the appropriate local authority and DfES are data controllers 'in common'. The local authority will take the lead in responding to Subject Access Requests made in relation to ContactPoint (see flowcharts at B8 & B9).

To comply fully with the request, relevant information from both the 'live' system and the archive should be provided. This will be available in the form of a standard subject access report.

4.8 **Making a subject access request**

A Subject Access Request can only be made by or on behalf of the individual that the information is about. ContactPoint holds information which is about children, about their parents/carers and about practitioners.

4.9 A Subject Access Request must be made in writing. It may specifically refer to ContactPoint or may be a broader request which can include ContactPoint data. The address for local authority Subject Access Request enquiries should be suitably publicised and sample wording should be made available to help in making such requests.

4.10 **Responding to a subject access request**

Local authorities have established procedures for handling Subject Access Requests which relate to information the authority is data controller for. In most local authorities there will be a Data Protection Officer who is responsible for ensuring these procedures are followed. These procedures should be applied to requests which include information held on ContactPoint.

4.11 In the interests of both the individual to whom the personal information relates, and the person handling the request, it is essential that information is only disclosed where the identity of the individual making the request is confirmed and their right to see the information is verified. The DPA contains a number of exemptions for circumstances in which personal information should not be released. These should always be considered.

4.12 Where a Subject Access Request is made in relation to a child's information there are a number of important considerations which must form part of the process of handling a request:

- **Sufficient Understanding** – As with consent to record sensitive services, a judgement must be made about whether a child has sufficient understanding to exercise their subject access rights. If so, they can make a Subject Access request or nominate a parent/carer to do so on their behalf.
- **Identity** - Documents which confirm the identity of the person making the request should always be sought. In the case of a parent/carer making a request, proof of the relationship with the child should also be sought.
- **Residency** – Proof of address should be sought from a person making a Subject Access Request and compared with the address listed for a child on ContactPoint. If they do not match, proof that the child is resident at that address (e.g. a GP's letter) should be sought. If a parent/carer cannot provide proof that they are resident with a child then legal advisors should be involved in determining whether to release information.
- **Court orders** – If a court order has been issued against a parent/carer then information must not be released. This may only be apparent after enquiries have been undertaken following the request. Any such request should be responded to with a clear statement that information cannot be provided under the terms of the court order.
- **Shielded information** – special consideration should be given to whether it is appropriate to release 'shielded' information or whether doing so may place the child at risk of harm.

4.13 **Correcting information**

Having made a subject access request, a data subject or their representative may identify inaccurate or out of date information on their record. If the local authority is satisfied that the information is indeed inaccurate or out of date, then it must correct the record. Where there is a dispute between the data subject (or their representative) and the local authority as to the accuracy of the data, the local authority should indicate on ContactPoint that a particular piece of information is disputed, the date of dispute and when the dispute was settled. Records of the details of the dispute must be kept locally - there is no facility to hold this on ContactPoint.

4.14 **Users**

If you receive a Subject Access Request relating to ContactPoint you should forward this to your LA ContactPoint Management Team.

If you do not work for a local authority, a Subject Access Request to see information held in your organisation's files will not include data on ContactPoint. Advice on handling such a request should be sought from your manager or data protection officer.

4.15 **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. Subject access requests which do relate to ContactPoint should then be directed to the appropriate ContactPoint manager.

4.16 **ContactPoint Management Team**

LA ContactPoint Manager - You should follow your local authority process for handling subject access requests, consulting your Data Protection Officer and legal advisors as appropriate. When it has been decided by your Data Protection Officer (or equivalent) that information from ContactPoint should be released in response to a SAR, you should produce a report to respond to the request.

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

4.17 **Complaints procedure**

ContactPoint Regulations set out specific requirements on local authorities regarding establishing and managing a complaints process covering the accuracy of data held and use of ContactPoint by authorised users within that authority.

4.18 The Regulations set out a number of specific conditions which local authority arrangements for handling complaints must meet. These are:

- there must be an identified complaints manager (this should usually be a member of the ContactPoint management team);
- complaints must be answered within 20 working days of their receipt;
- the procedure for making a complaint is set out in writing and made freely available (for instance by displaying in waiting rooms, including in materials produced to explain ContactPoint and placing on authority websites); and
- that any complaint made within one year of the issue occurring must be handled. The complaints manager may investigate older complaints if they judge that it would not have been reasonable to expect the complaint to be made within the one year time limit.

As long as these conditions are met, local authorities may choose to integrate arrangements for handling ContactPoint with existing local procedures for handling complaints.

4.19 Local authorities are not responsible for all complaints which relate to ContactPoint. ContactPoint regulations set out the following exclusions from local authority responsibility to handle complaints:

- any action, decision by the Secretary of State or about the Regulations, guidance or directions issued under section 12 of the Children Act 2004. These should be directed to the DfES;
- other local authorities in relation to the operation of ContactPoint;
- complaints about any action or decision made by a practitioner who has access to ContactPoint;
- a complaint about a national partner organisation;
- a complaint by a local authority employee in relation to a contract of employment;
- a complaint by a local authority contractor in relation to their contract;
- a complaint in relation to subject access rights under the Data Protection Act;
- a request for information under the Freedom of Information Act; or
- a complaint where the complainant has indicated in writing that they intend to instigate legal proceedings.

Where a complaint is received for which a local authority is not responsible, this should be directed to the appropriate organisation or body. In the case of complaints relating to Subject Access Requests or requests under the Freedom of Information Act, these should be handled by the data protection officer or the local authority in line with existing procedures. All partner organisations should have existing complaints procedures in place which can be used to address these complaints.

4.20 In cases where a complainant does not feel that their complaint has been handled satisfactorily the local authority may have a review process. If there is not a review process, or the outcome of a review is not satisfactory there is further recourse in some circumstances:

- The local government ombudsman can investigate complaints relating to ContactPoint use and users;

- The Information Commissioner can investigate complaints where these relate to the accuracy of ContactPoint data.

4.21 **ContactPoint Management Team**

LA and partner organisation ContactPoint managers – You must ensure that there are arrangements in place within your organisation as set out in the Regulations and based on the guidance above. Your complaints procedure must be accessible to children as well as adults. Local authorities must include information about their complaints procedure in materials they produce to promote and explain ContactPoint (see 3.53-3.57).

4.22 **Reporting and management information**

Reports support the functions of ContactPoint and the management of system and users. There are three types of report - strategic, operational and technical. Access to ContactPoint reports is based on having the appropriate access rights. New types of report can only be created by the central (national) ContactPoint team.

4.23 Requests may be made under the Freedom of Information Act 2000 (see A16), which relate to operational data held on ContactPoint. Local authorities can handle requests relating to their 'compartment' of the system. Any requests which relate to national or regional information should be passed to DfES and the central (national) ContactPoint team. Information must be provided unless it is exempted by one of the Freedom of Information Act exemptions or exceeds the acceptable cost threshold for responding to requests. Organisations will have procedures in place for compliance, and should manage such requests on a case-by-case basis.

4.24 **ContactPoint Management Team**

LA and partner organisation user account administrators – You should use the appropriate reports to support your responsibilities for reviewing ContactPoint usage. This includes regularly (for instance weekly) viewing reports of the ContactPoint audit trail to identify and follow up any possible misuse (see 3.9-3.12).

LA ContactPoint managers and data administrators – 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.

4.25 **Partner organisations administering user accounts**

Local authorities can allow local or regional partner organisations to administer user accounts for their employees or those engaged to provide services to the organisation. This is done by granting user account administrator rights to appropriate individuals in the partner organisation.

4.26 These individuals can then carry out several administrative functions. This includes nominating individuals for user accounts, maintaining user account information (including resetting passwords), auditing usage (if appropriate) and suspending/closing user accounts. These user account administrators can only create a new user account for an individual if the local authority ContactPoint team determines that this is appropriate. The conditions for access to ContactPoint remain unchanged.

4.27 **Suspending/removing user account administration**

The local authority which granted user account administration rights to a partner organisation has overarching responsibility for all users in its area. The LA ContactPoint management team has the facility to suspend and remove user account administration rights from a partner organisation if this becomes necessary.

4.28 **ContactPoint Management Team**

LA ContactPoint Managers - You remain responsible for determining that individuals nominated by partner organisations are eligible for access. You should only authorise the creation of a new user account where you are satisfied that the relevant conditions are met (See 2.7). You should periodically monitor the usage of these users to identify any suspicious usage or potential misuse (See 3.9 & 3.12).

Where you believe that misuse or unauthorised activity is being carried out by users administered by a partner organisation, you may suspend their user accounts and together with the partner organisation, carry out an investigation.

If you are concerned that partner organisation user account administrators are not administering their users correctly, you should investigate immediately. You may take over managing their users and suspend or remove the user account administration rights as appropriate.

4.29 **Creating a new ContactPoint user account**

There are 5 conditions of access that all applicants must satisfy before being granted a user account (See 2.7).

4.30 A judgement must be made based on the information in their enhanced CRB The requirement to have an enhanced CRB disclosure which is renewed every three years is specific to ContactPoint and does not replace existing organisational policies for non-ContactPoint users. Individuals who do not have an enhanced CRB disclosure or have one which is more than 3 years old will have to apply for a new disclosure to become ContactPoint user. Applications for enhanced CRB disclosures should be made in sufficient time to receive it before access is needed (or a previous disclosure reaches 3 years). If evidence of a renewal is not received before the 3 year period the user account may be suspended. The fact that an applicant has a criminal record does not automatically make them unsuitable to have access. Certain

convictions are particularly relevant to this judgement. In addition to any convictions which relate to offences against children, offences under the Computer Misuse Act 1990 or the Data Protection Act 1998 should be considered carefully. The Department cannot advise whether a particular person is suitable for access, this judgement should be made by the applicant's employer or the ContactPoint Management Team.

4.31 A ContactPoint account should only be created once all of the conditions are met (see 2.7). Where a partner organisation requests a user account (except for national partner organisations specified in ContactPoint regulations to manage their own users), the local authority makes the determination whether this account should be created. The account should be established with the appropriate access rights to ContactPoint functions.

4.32 Access to ContactPoint should be subject to review. When an authorised user changes their position within an organisation, or their job description changes, this should trigger a review of whether it is still necessary for them to have access.

4.33

ContactPoint Management Team

User account administrator - You must only create a user account and issue a security token when an applicant has met all of the appropriate conditions (See 2.7).

Before creating a user account 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 3 years old. The employer must also confirm that, on the basis of this disclosure, they judge the applicant to be suitable to have access to ContactPoint.

All users must have completed an approved ContactPoint training course based on the national training materials. They must also have received any other training your local authority (or national partner), considers appropriate. This should include information sharing training, preferably based on the national materials (see C25) so that user understands the principles of information sharing. Your authority should consider making 'refresher' training available where individuals have previously completed relevant training. Your authority is responsible for providing the necessary training to users from the local area.

Partner organisation user account administrators - You may only nominate employees of your organisation, or those engaged to provide services to your organisation as ContactPoint users.

4.34 **Suspending a ContactPoint user account**

Suspension of a user account is the temporary removal of access rights without permanently closing the account. If the account is suspended, it will not be possible to access ContactPoint by any method, including mediated

access.

4.35 The ContactPoint Management Team should usually be responsible for suspending accounts. A request from another source to suspend an account should be verified with the requestor and a written record should be kept of the reasons for each suspension. The central (national) ContactPoint team can suspend the accounts of any user or groups of users.

4.36 The ContactPoint management team may decide to suspend a user account for a number of reasons, including:

- where a user is known to be going on extended leave (e.g. secondment, maternity, sickness), and not need ContactPoint access;
- where potential suspicious activity has been identified (See 3.9-3.12);
- during an investigation into usage of ContactPoint;
- where a user is found to be not adhering to any significant aspect of this guidance;
- due to prolonged inactivity of an account;
- if the user is suspended by their employer, for any reason; and,
- where a user's enhanced CRB disclosure was issued more than 3 years earlier and renewed disclosure has not been provided.

4.37

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 for them to arrange for your account to be suspended.

If you account is suspended whilst an investigation is carried out, you must assist in any investigation which is undertaken. You must not attempt to access ContactPoint whilst your account is suspended.

4.38

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 should cooperate with this investigation.

4.39

ContactPoint Management Team

If one of the situations listed above 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.

You should 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 should be kept of all investigations and any

decisions which are made.

4.40 **Closing a ContactPoint user account**

When any user no longer needs or should no longer have access to ContactPoint, their user account must be closed. This should be done by their user account administrator.

4.41 **Staff Managers**

If a ContactPoint user leaves their job or changes their role, and no longer requires access, you must inform the user account administrator before the staff member leaves/changes role. This will ensure that their account is closed on the correct date. The user's security token must be returned to the user account administrator when they no longer need it

4.42 **ContactPoint Management Team**

LA and partner organisation user account administrators - 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. When accounts are closed you should recover the security token, if this cannot be recovered you must ensure that this token cannot be used to access ContactPoint. You should periodically review user accounts which appear to be dormant and suspend or close accounts as appropriate.

4.43 **Audit of ContactPoint usage**

All activity on ContactPoint is continuously recorded in an audit trail. This includes searches and access to child records; national, regional and local data uploads; and practitioner involvement and amendments. This audit information can be reviewed to establish what has occurred on ContactPoint, how it has been used, and by whom.

4.44 **ContactPoint Management Team**

LA ContactPoint Managers - You are responsible for ensuring that all activity by users in your area is monitored.

4.45 **Establish a local data feed**

Local authorities are responsible for managing local data supply arrangements between local organisations and ContactPoint. These arrangements can only be made with a person or body '**required'** or '**permitted'** to supply information, under Section 12 of the Children Act 2004 and Regulations (see C.22 & C23).

4.46 Before a data source is connected to ContactPoint, it must be accredited. This ensures that the data is supplied according to the ContactPoint security policy, does not disrupt the operation of ContactPoint and does not degrade data quality. Data sources which do not meet the accreditation standards

cannot provide data to ContactPoint.

4.47 The accreditation process will not be able to determine the degree to which data is accurate (e.g. a child actually lives at the address given). Accuracy will be addressed further in ContactPoint support and training materials. Local authorities should also consider the accuracy of a potential data source when considering establishing a new data supply agreement.

4.48 **ContactPoint Management Team**

LA data managers – Where you identify an appropriate source of data you will be responsible for making the necessary arrangements for that data supply to ContactPoint - a 'data supply agreement'.

You should consider a number of factors when deciding if a potential local supplier is appropriate to provide data to ContactPoint. These should be considered early in the process of establishing a new local data feed. The factors are:

- Whether the organisation already provides data at a national level;
- Whether the data will add value to ContactPoint; and
- Whether the quality of the source data meets ContactPoint accreditation standards.

Further advice is available on assessing potential local data sources, arranging suitable agreements to manage data sharing and making the necessary arrangements to connect a local data supplier can be found in support materials for local authorities.

4.49 **Terminating a local data supply agreement**

A local data supply agreement can be suspended or terminated by the local authority at any time if it is decided that this is necessary.

4.50 **ContactPoint Management Team**

LA data managers – You must regularly review all local data feeds to identify any data supply issues. You should 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.

4.51 **Data matching and data cleansing**

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.

Data cleansing is the task of correcting or removing duplicate, inaccurate or mismatched data. Data cleaning is an ongoing process.

4.52 **ContactPoint Management Team**

LA data administrators – You are responsible for data matching and cleansing for records in your compartment of ContactPoint. These activities must be carried out on a regular basis, and any discrepancies followed up. You should use the ContactPoint data management functions to support this activity. The team must match this data to an existing ContactPoint record, create a new record, or report back to the source data controller that the data is not usable. You must aim to meet any data matching and cleansing targets which are set for you by the National (Central) ContactPoint Team.

4.53 **Child moves between local authorities**

The local authority responsible for a child's record is determined by where the child is understood to be 'ordinarily resident' (see G*lossary*). It is not always known where a child is ordinarily resident. In order to ensure that each child record is the responsibility of a single local authority, all records will be automatically assigned to a local authority by ContactPoint based on the available information when they are first created.

4.54 When a child moves from one local authority to another their record should also be transferred. Where the record only has universal services listed this will be done automatically by ContactPoint. Where there are specialist/targeted services on a record, the old and new local authorities must both agree to a transfer before responsibility for a record is moved and ensure that the relevant practitioners are made aware of the transfer.

4.55 Local authorities can only move responsibility for a record where another authority is identified as the suitable recipient and agrees to the transfer (i.e. when a child moves).

4.56 When determining which local authority a child record should be assigned to, the following should be borne in mind:

- Where the child is known to be ordinarily resident in one authority the record should be assigned to this authority;
- Where the child lives in more than one authority the record should usually be assigned to the authority in which the child lives for the greater proportion of time;
- Where there is an existing responsibility for provision of services (such as the council with social services responsibility) the record should usually be assigned to this authority; and
- Where there is a dispute this must be sorted out between local authorities and the record can only be transferred with the agreement of both authorities.

4.57 Highly mobile children and families may move frequently within and between local authorities. Where an authority is identified to lead on the provision of services, for example where a child from Gypsy, Roma or Traveller family has a base school, this local authority should retain responsibility for the ContactPoint record. Where there is no identified lead authority, the child record should remain with the authority to which it is assigned by ContactPoint until a more suitable authority is identified and both authorities agree to transfer the record.

4.58 Where a local authority does not believe it should be responsible for a record which is assigned to it, it should identify the local authority which it believes should be responsible and propose a transfer.

4.59 **ContactPoint Management Team**

LA ContactPoint managers – You are responsible for ensuring that records are transferred to and from your authority as appropriate. This will be a regular task and you should use reports to support this activity.

Child records with only universal services will be transferred automatically based on available information. You will only have to take actions relating to records with specialist/targeted services or where it is necessary to override the automatic transfer process. You can propose a transfer to or from another authority and accept or reject transfers proposed by other ContactPoint managers.

Where there is uncertainty over which local authority should be responsible for a child record, you should discuss and resolve this with the other relevant ContactPoint manager/s. You may wish to contact service providers listed on the child record to assist you in determining the appropriate compartment for the child record.

4.60 **Child leaves England**

When a child is believed to have left England and has no intention of returning (e.g. where the family has emigrated) the local authority that holds the child record is responsible for archiving it. Reasonable steps must be taken to confirm this before the child record is archived.

The child's record will remain in the archive for six years, after which it will be deleted. If the child returns to England, the child record can be restored to the live system from the archive by any ContactPoint Management Team.

4.61 **Users**

When you are informed a child leaving England permanently you should inform the ContactPoint Management Team accordingly.

If you come into contact with a child who has recently returned to England (having been out of England for less than 6 years) and you cannot find a child record on ContactPoint there may be a record in the archive. You should contact the ContactPoint Management Team to allow them to search the archive and, if possible, restore the child record.

4.62 **ContactPoint Management Team**

Data administrator - Where a practitioner believes that a child may have returned to England (having been out of England for less than 6 years), you must carry out a search of the archive. If you identify the child's record, it

must be restored to the live system.

If you are successful in restoring the record, you should inform the user to ensure that they do not attempt to create a new record.

4.63 **Shielding records**

ContactPoint has the facility to hide from view or 'shield' data from ContactPoint users. The use of this facility is determined on a case-by-case basis. There are limited circumstances where this would be applicable, chiefly these are when there are strong reasons to believe that by not doing so is likely to:

- place a child at increased risk of significant harm;
- place an adult at risk of significant harm;
- prejudice the prevention or detection of a serious crime; or,
- provide a link between pre- and post-adoption identities.

4.64 Shielding instructions may come from ContactPoint data sources. Where a record is shielded on a source system this shielding will also be applied to the ContactPoint record. Practitioners who are users can send a shielding notification to the LA ContactPoint manager where they judge that a child record must be shielded. Practitioners who are not users should contact the LA ContactPoint manager when they believe that a record should be shielded. A child or parent/carer may request that a record is shielded by discussing this with a user (who then sends a notification) or by contacting the LA ContactPoint manager.

4.65 Searches for records containing shielded data will only show minimal information, and none which will identify the child's whereabouts or locality. Further information will only be available from the relevant LA ContactPoint Management Team who will decide on a strict case-by-case basis, taking further advice where necessary, whether it is appropriate to provide information.

4.66 To ensure that this facility is used appropriately, shielding decisions should be reviewed at regular intervals by a local authority shielded record panel. This panel should seek views from relevant practitioners and, if appropriate, the child and their parent/carers when deciding whether a child record should remain shielded. Only the LA ContactPoint manager can unshield records. This is only done where all sources of shielding notifications no longer advise that a record requires shielding.

4.67 **Users**

You must act promptly if you have strong reasons to believe that there is a risk of significant harm or a serious crime if the information remains visible to authorised users on ContactPoint. You should discuss this, where appropriate, with the child and/or their parent/carer. A child or their parent/carer may request that a record is shielded, you should judge if this is appropriate. 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. If the situation is urgent you can mark a record for shielding on ContactPoint which will ensure that it is instantly shielded.

4.68 **Staff Managers**

You should discuss with those you manage, the appropriateness of shielding a child record on ContactPoint. You should also be prepared to support the user in considering the need for continued shielding, when this is reviewed.

4.69 **ContactPoint Management Team**

LA ContactPoint managers – Where a request to shield a child record is made to your team, from any source, it should be carried out as a matter of urgency. The decision to shield should be based on the reason for the request, the views of practitioners working with a child, and unless inappropriate, should be discussed with the child or their parent/carer.

Your local authority should convene a shielded record panel at regular intervals (for instance quarterly) to review shielding decisions. This panel should periodically review all active shielding decisions. The panel should include members with appropriate practical experience (e.g. child protection officers, social workers who handle cases of domestic violence). This review should take into account the views of the child and/or their parent/carer, if appropriate, and of practitioners who work with the child, particularly those who have requested shielding. A record should only be unshielded where all of the sources of shielding notifications confirm that shielding is no longer required.

4.70 **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.

4.71 In cases where a new identity is created, ContactPoint must not allow a link between the old identity and the new identity. This can be done by immediately moving the child record for the old identity to the archive and then creating a new child record using the new identity.

4.72 **Users**

You must not attempt to use ContactPoint in order to discover details of a new identity for a child or the former 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 old identity you should inform the ContactPoint Management Team.

4.73 **ContactPoint Management Team**

LA ContactPoint manager – You are responsible for managing records associated to a child's old identity. You may also be asked to establish a new child record for the new identity – you must ensure that the record for the child's previous identity is moved to the archive before the new child record is created.

4.74 **The archive**

Information is held in the archive for a period of 6 years from the date on which it was archived. This period of retention can be extended for a limited period in cases where there is an ongoing (or planned) investigation relating to the child. Information in the archive can only be accessed by the central (national) ContactPoint team and the LA ContactPoint Management Teams.

4.75 **Closing and archiving records**

Entire records are closed and moved to the archive when:

- A child leaves England and the local authority in which the child last resided decides that the child will not return (If the child returns within 6 years it is possible to reinstate the record);
- A child reaches age 18, unless consent has been secured to hold the child record after this date and the child is leaving care or has learning difficulties;
- Consent to retain a child record for an over 18 year old leaving care or with learning difficulties is withdrawn or when the period of extended retention is completed (up to the maximum of 25);
- A child is given a new identity which must not be linked to the old identity; or
- One year after the death of a child is confirmed by information from the Registrar General (See 3.37).

4.76 Information within a child record (for instance service involvement) can be archived, without the entire child record being moved to the archive one year after involvement has ceased. Practitioners can extend the retention of this information for up to 5 years where they judge it appropriate (see 3.42).

4.77 Where a child moves to Scotland or Wales but continues to access services in England their child record must still be moved to archive as there is only legal power for ContactPoint to hold records for children who are resident in England. This should be done by the local authority in which the child was last ordinarily resident.

4.78 **Retrieval from the archive**

For a limited number of reasons archived records can be accessed for a limited period or they can be restored to the live system and made visible to authorised users.

4.79 The reasons for which the records will be accessed or restored are:

- Where a child record was archived when they left England, but the child returns to England within 6 years and before their 18th Birthday;
- 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 A.8);
- Serious case reviews and unexpected child death investigations, carried out by a Local Safeguarding Children Board;
- The investigation of a complaint arising out of ContactPoint operation;
- Where a particular and compelling reason to reinstate the archive has been demonstrated to the central (national) ContactPoint team.

4.80 **Users**

When the period of retention for an involvement with a child is reached your contact details will pass into the archive. This information will not be accessible to other users and will only be accessed in the limited circumstances listed above.

4.81 **ContactPoint Management Team**

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 you may extend the period of retention beyond the 6 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.

Annex A - LEGISLATION

This chapter offers only a brief outline. You should not use this chapter as a substitute for reference to the legislation itself. This chapter identifies legislation relevant to ContactPoint:

- the legislative basis for ContactPoint (A1);
- the legislative purpose ContactPoint (A2);
- other relevant legislation (A7).

A1 Legislative basis of ContactPoint

Children Act 2004

Section 12 of the Children Act 2004 covers 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.

The Children Act 2004 Information Database (England) Regulations 2007, made under the Children Act 2004 Section 12, cover:

- the specific information to be included on ContactPoint;
- arrangements for ensuring accuracy of the information held;
- the persons or bodies required or permitted to supply data to ContactPoint;
- the types of users who may be granted access to ContactPoint;
- the conditions of access;
- the length of time information can be retained on ContactPoint; and
- the requirement for LAs to establish a complaints procedure.

A2 Legislative purpose of ContactPoint

ContactPoint may only be established and operated for purposes which support certain duties specified in legislation, chiefly sections 10 and 11 of the Children Act 2004 and section 175 of the Education Act 2002.

A3 Children Act 2004

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

- physical and mental health, and emotional wellbeing;
- protection from harm and neglect;
- education, training and recreation;
- making a positive contribution to society;
- social and economic wellbeing.

A4 **Section 11** imposes a duty on key people and bodies to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children. This duty requires organisations to:

- carry out their existing functions in a way that takes into account the need to safeguard and promote the welfare of children; and
- ensure that the services they contract out to others are provided having regard to that need.

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.

A5 Education Act 2002

Section 175 imposes a duty on LAs, and the governing bodies of maintained schools and further education institutions to make arrangements in regard to the welfare of children. LAs must make arrangements to ensure that their functions in the capacity of an LA are exercised with a view to safeguarding and promoting the welfare of children. Similarly, governing bodies must make arrangements to ensure that their functions relating to the conduct of the school, or institution, 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.

A6 Education and Inspection Act 2006

Section 4 amends the **Education Act 1996** by inserting section 436A, which imposes a duty on LAs 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), children in their area who are of compulsory school age but who are not on a school roll, and who are not receiving a suitable education otherwise than by being at school (for example, at home, privately, or in alternative provision).

A7 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.

A8 Children Act 1989

Section 17 - Provision of services for children in need, their families and others – it is the general duty of every local authority to safeguard and promote the welfare of children within their area who are in need; and 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 – Says that the local authority, for assistance in the exercise of its statutory functions (which include the provision of services for children in need and the sharing of information for these purposes) request the help of any local authority, local education authority, health authority and any person authorised by the Secretary of State.

Section 47 - Local authority's duty to investigate – where a local authority has reasonable cause to suspect that a child who lives/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.

A9 Safeguarding Vulnerable Groups Act 2006

This Act establishes a Vetting and Barring Scheme (VBS) for those working with children and vulnerable adults. When the scheme is operational (Autumn 2008), ContactPoint users will be subject to the VBS requirements in addition to obtaining an enhanced CRB disclosure (or equivalent for police users). Further detail on the VBS and the requirements for ContactPoint will be provided to local authority ContactPoint Management Teams.

A10 Computer Misuse Act 1990

This Act provides, amongst other activities, that 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 2 years and a fine of up to level 5 on the standard scale (currently £5,000).

A11 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. The main requirements of these concern the fair and lawful obtaining of personal information, data quality and security.

One of the keys to complying with the principles is to ensure that the subjects of information are aware that you hold information about them, and what the information will be used for. Information should not be used in a way that people are unaware of or would not expect. Explanatory leaflets can be used to ensure that this is not the case.

A12 The DPA also gives a set of rights to individuals. These include a legal right of access to personal information. Individuals also have a right to have incorrect information put right.

A13 The DPA also provides that a serious offence is committed where personal data is unlawfully obtained or disclosed without the consent of the data controller. The penalties for an offence under the Data Protection Act are a fine up to level 5 on the standard scale (currently £5,000).

A14 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.

A15 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 applies to information held on ContactPoint. The enquirer is entitled to be told whether the authority holds that information and, if so, to have access to that information. If any part of the request includes information which can identify individuals, then this information will not be released, either by editing out the identifying data (redaction), or withholding the information. The Act recognises the need to preserve confidentiality and protection of sensitive information in some circumstances and these are listed in the Act as exemptions.

A16 The Human Rights Act 1998 and the European Convention of Human Rights

Article 8 of the European Convention on Human Rights (incorporated under the Human Rights Act 1998) recognises a right to respect for private and family life.

Sharing confidential information may be a breach of an individual's Article 8 right: the question is whether sharing information would be justified under Article 8.2 and proportionate. The right to a private life can be legitimately interfered with where it is in accordance with the law and, for example, is necessary for the prevention of crime or disorder, for public safety or for the protection of health or morals, or for the protection of the rights and freedoms of others. You must consider the pressing social need and whether sharing information is a proportionate response to an identified need and whether this would override the individuals' right to privacy. (Further Guidance is available in *Information Sharing: Further Guidance on Legal Issues, paragraphs 2.1-2.3).*

Annex B - FLOWCHARTS

These flowcharts support a number of the processes covered in this guidance. They are intended as a guide and are not definitive. There may be established processes within your organisations which cover or can be adapted to cover or join up with these, which you may wish to follow.

B1 Colour Codes

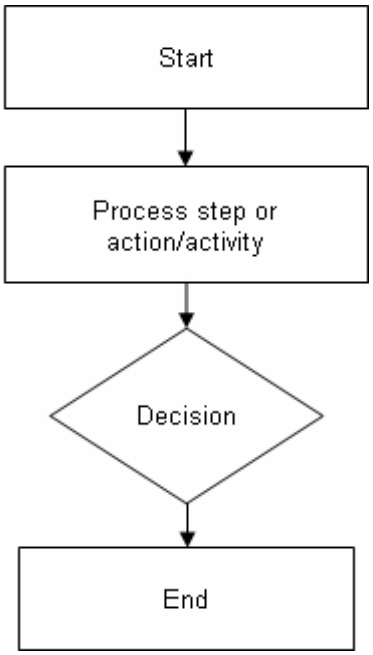
The flowcharts follow the colour-coding established in the table at 1.13, and used throughout this guidance. Two further groups are introduced for the purposes of these flowcharts. The process step types are identified by shape and are defined below.

Public: Child or Parent/Carer

ContactPoint User: Practitioner, manager or administrative/support staff

Staff Manager: Manager in organisation but non-ContactPoint user

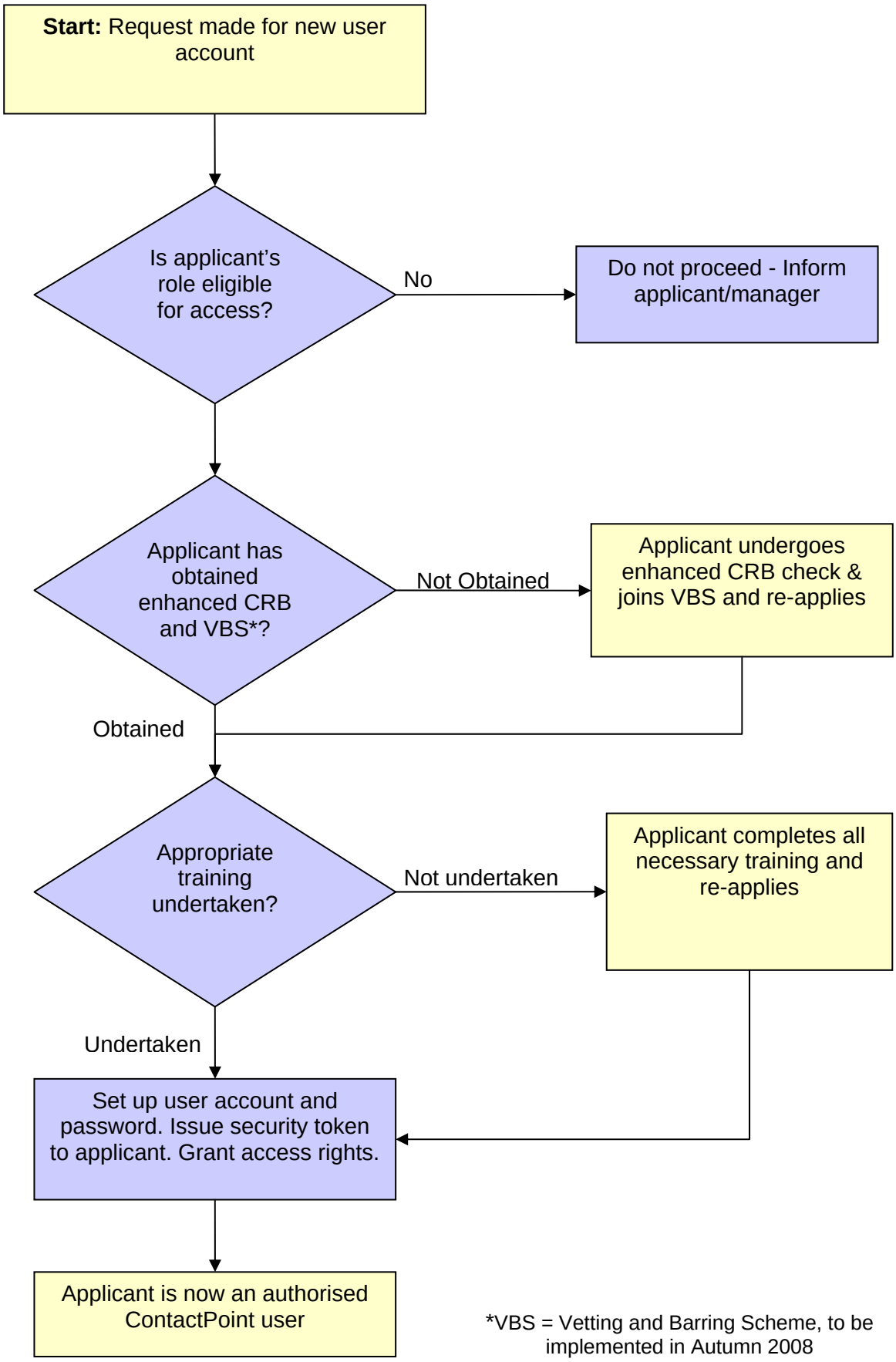
ContactPoint Management Team: Manager, User account administrator or Data administrator



B2 References are made between the relevant sections and flowcharts throughout the guidance

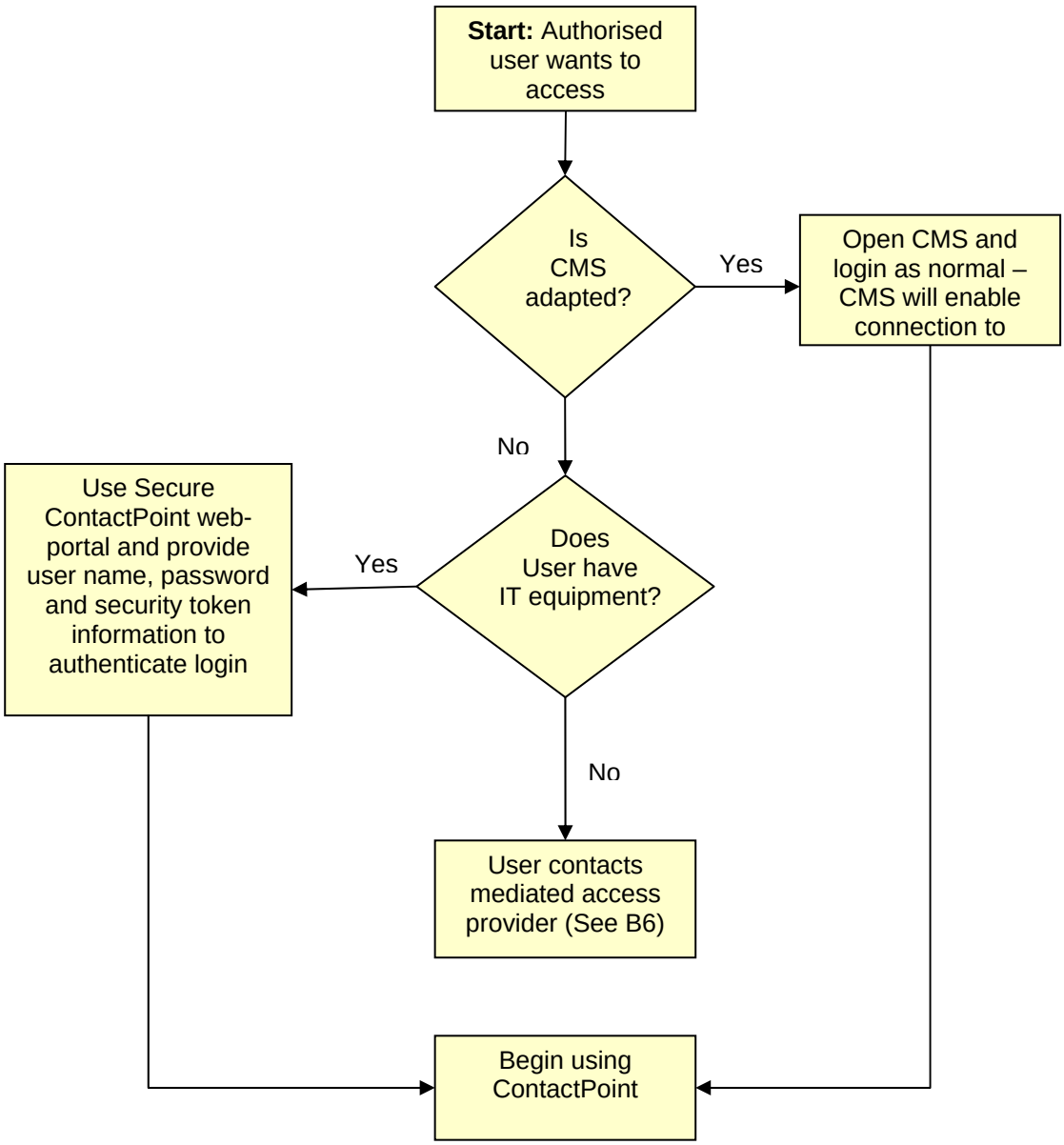
B3 Records of all action taken and decisions made must be recorded by the relevant staff. In some cases this will include both non-ContactPoint users and ContactPoint Management Team staff.

B4 Creating a new ContactPoint user account (See 4.29-4.33).

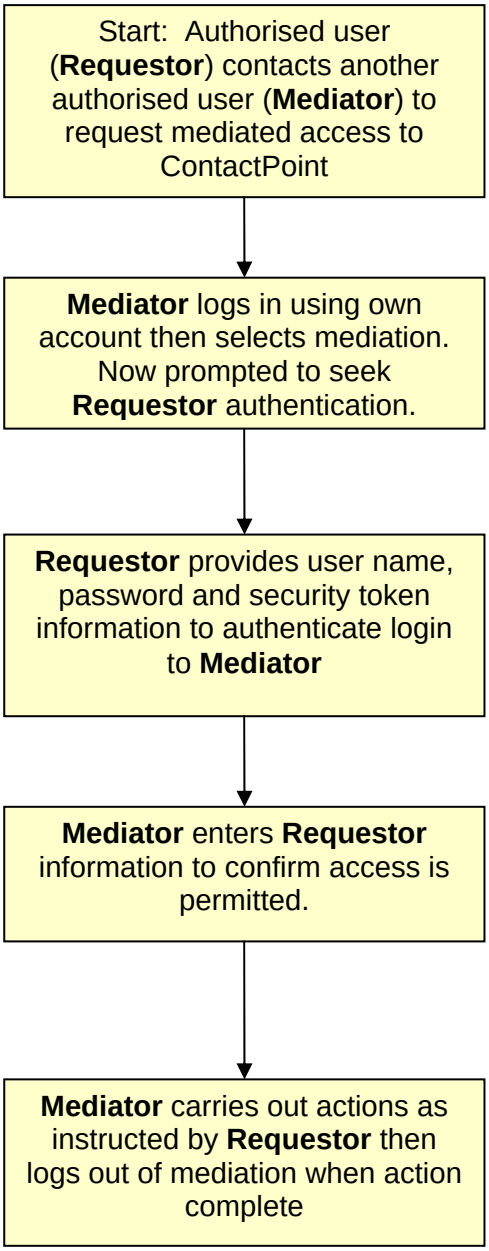


*VBS = Vetting and Barring Scheme, to be implemented in Autumn 2008

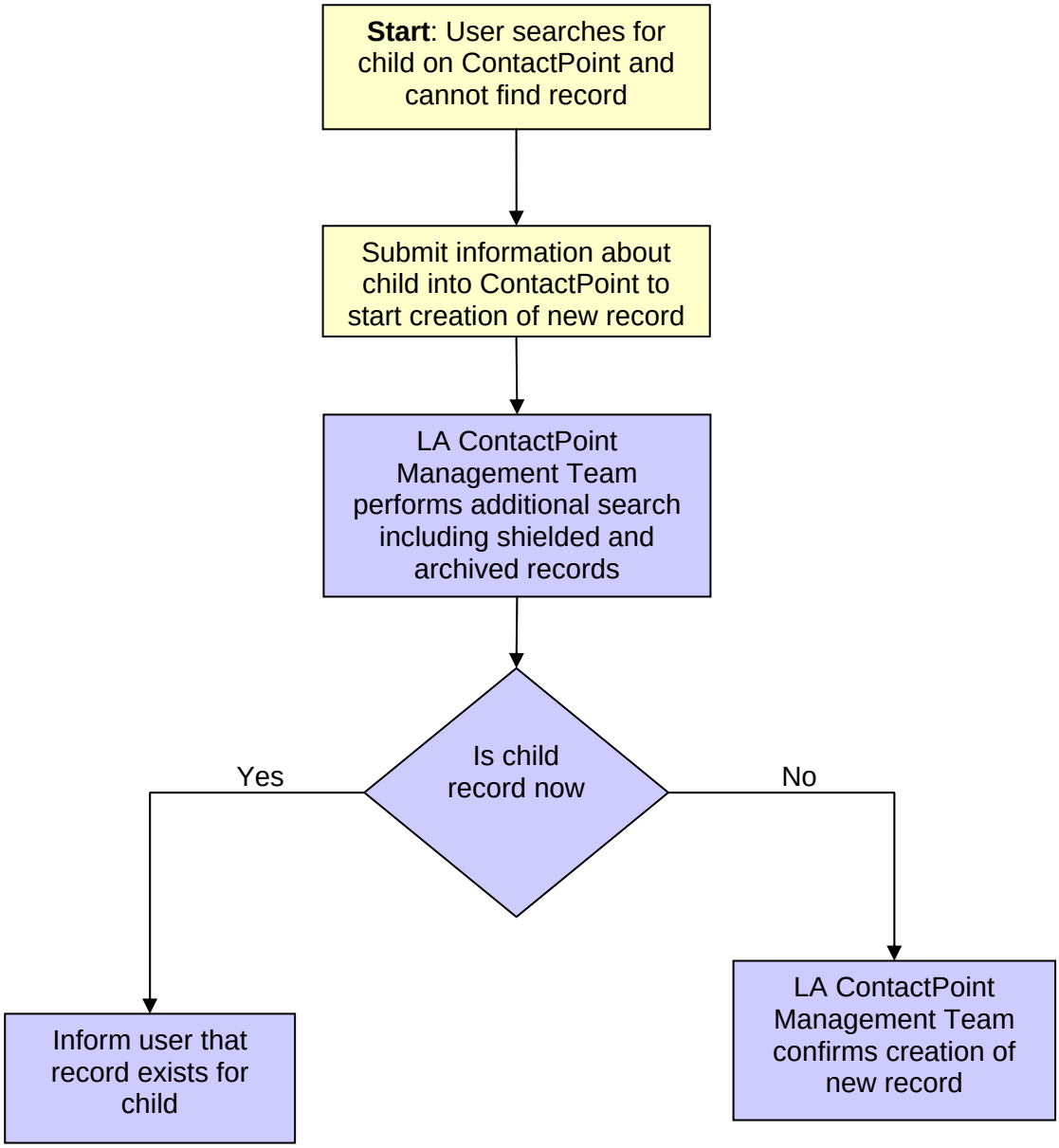
B5 User Access (Direct) See 2.11-2.13.



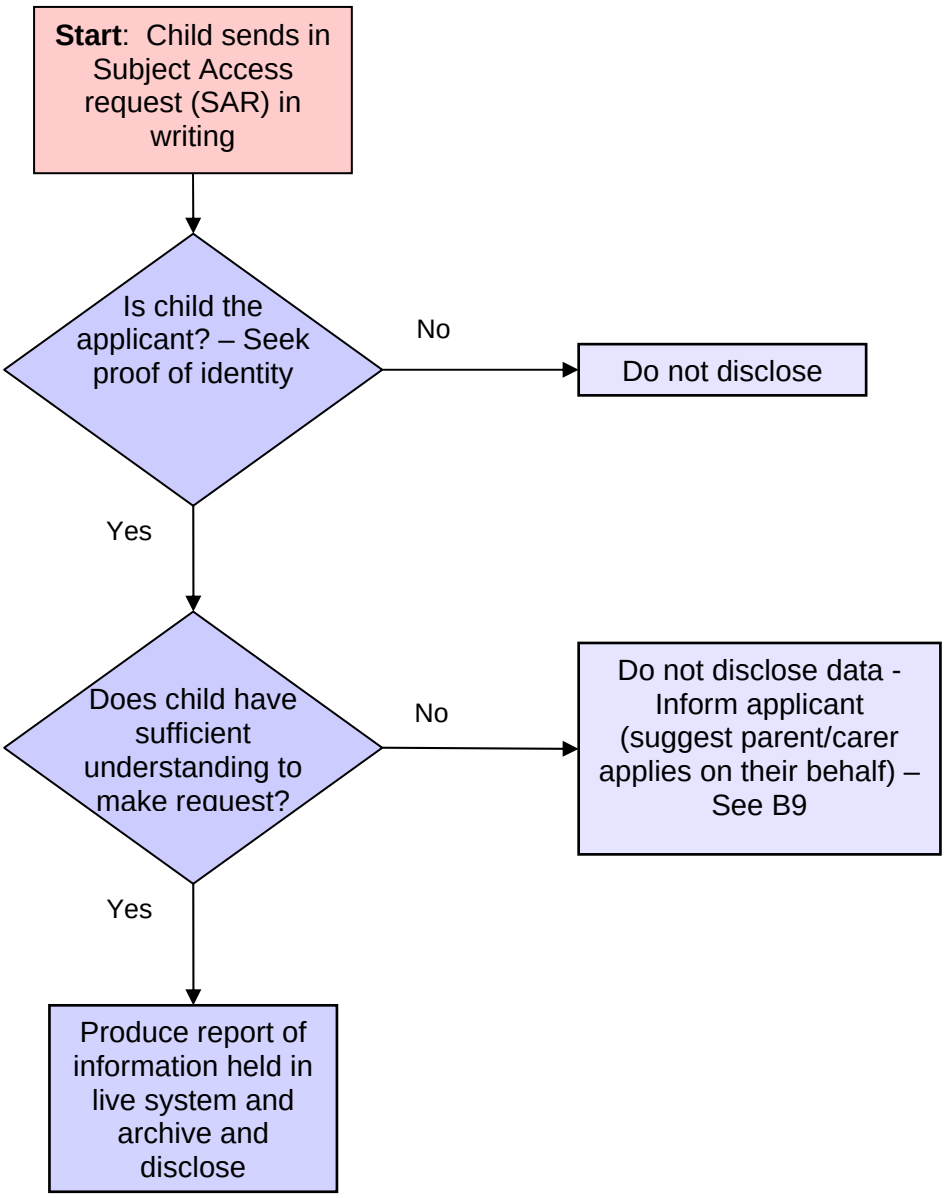
B6 User Access (Mediated) See 2.14-2.16



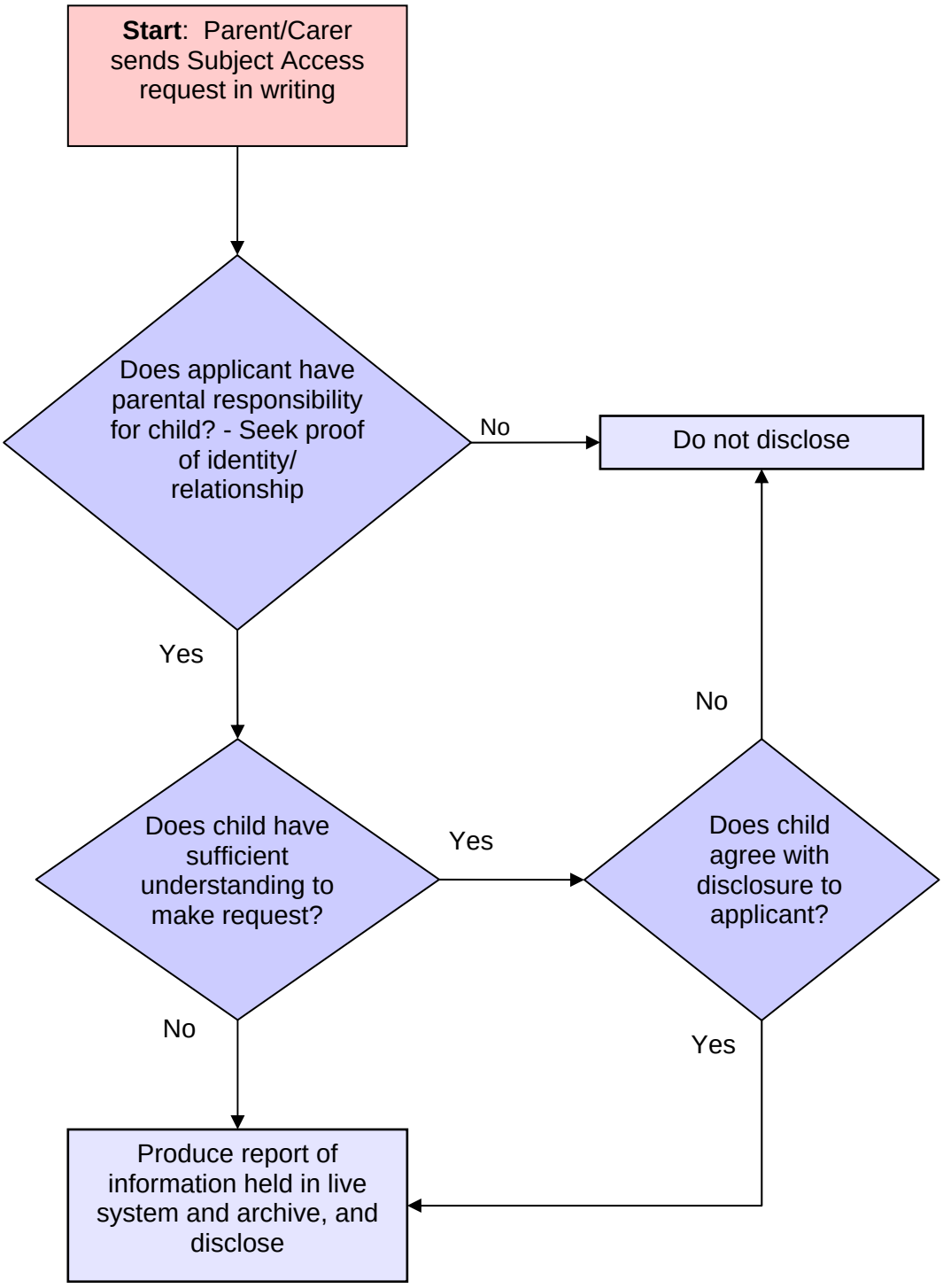
B7 Manually requesting/creating new child record (See 3.19-3.22)



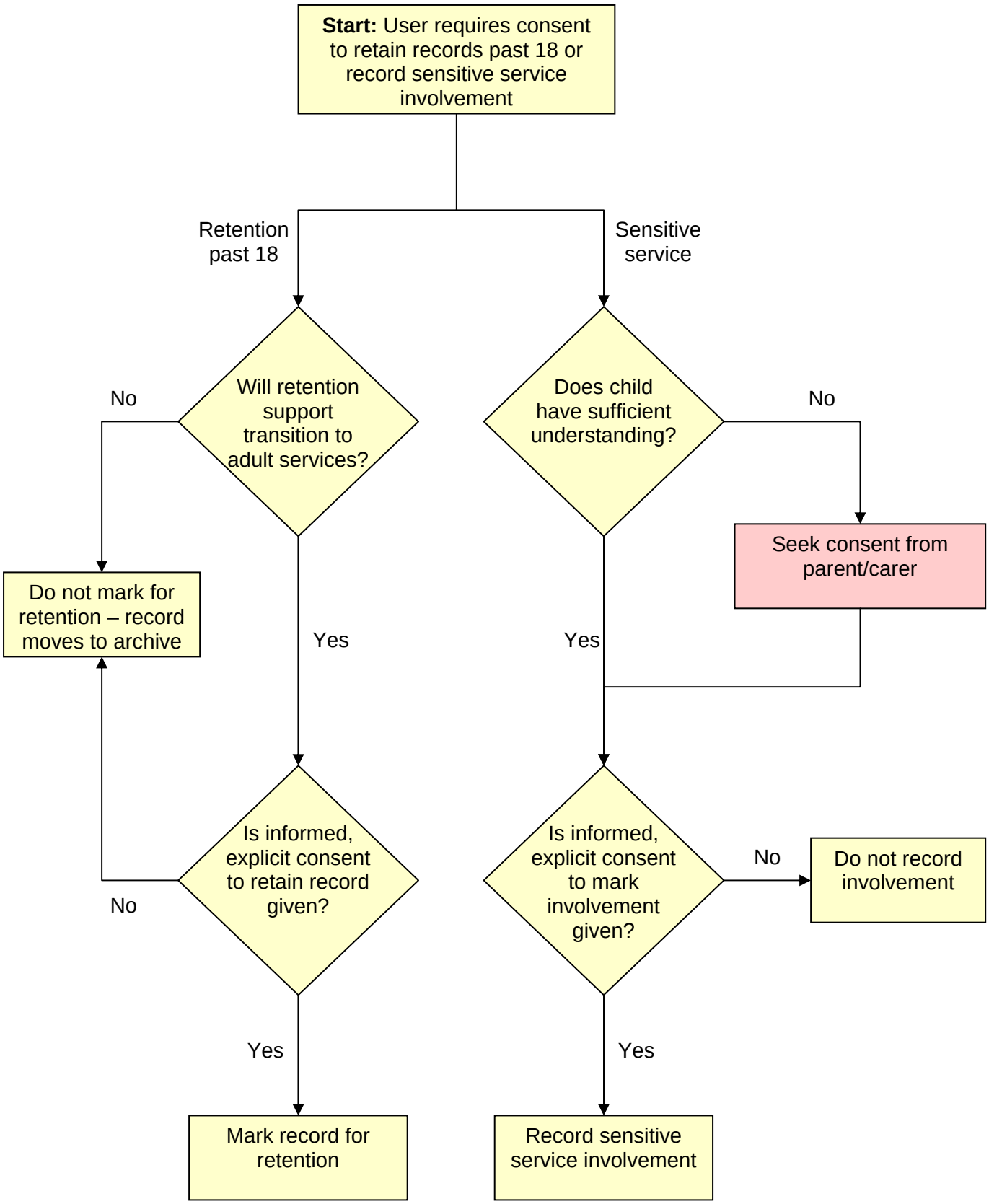
B8 Subject Access Request by Child (See 4.7-4.16)



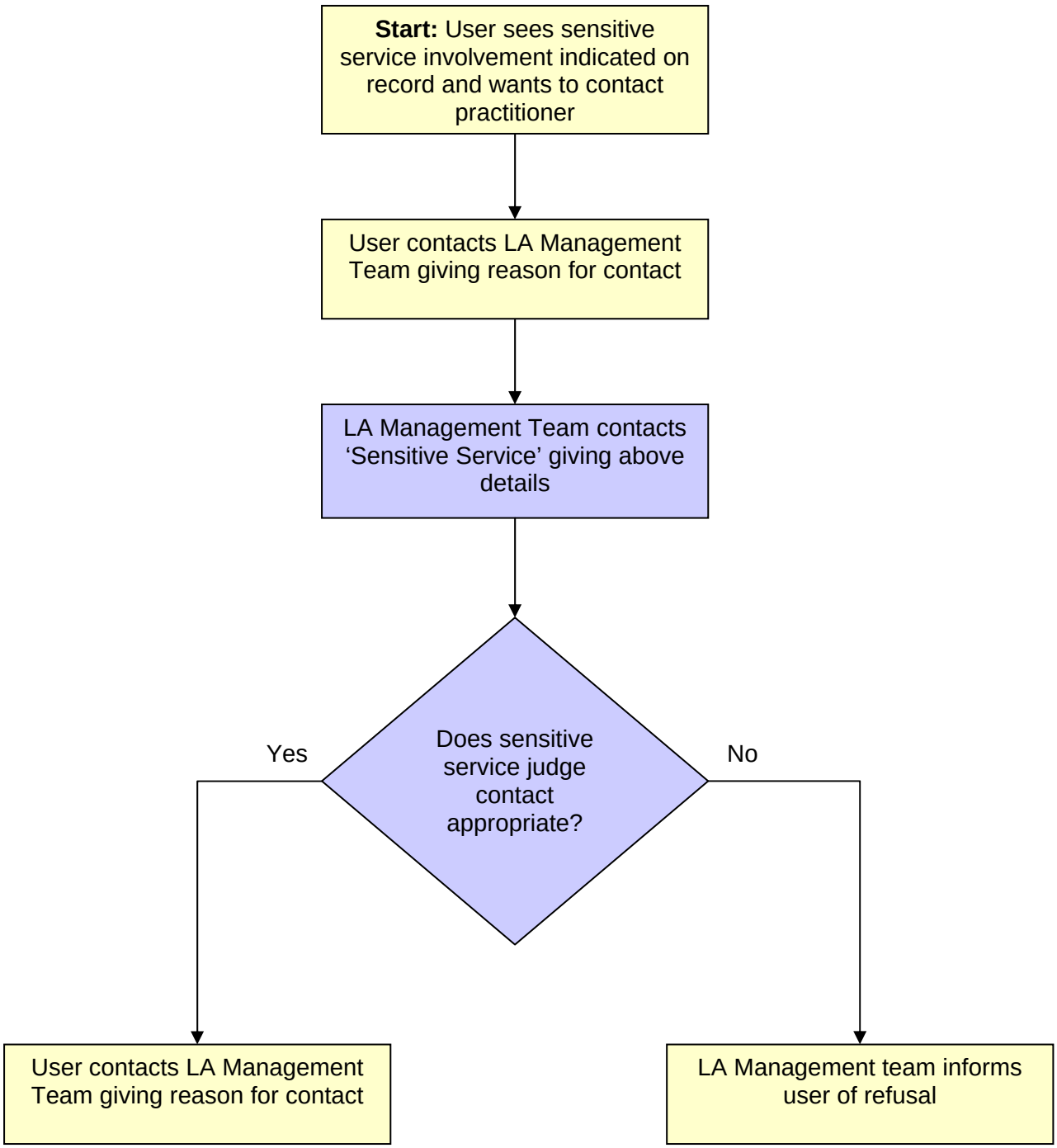
B9 Subject Access request on behalf of a Child (See 4.7-4.16)



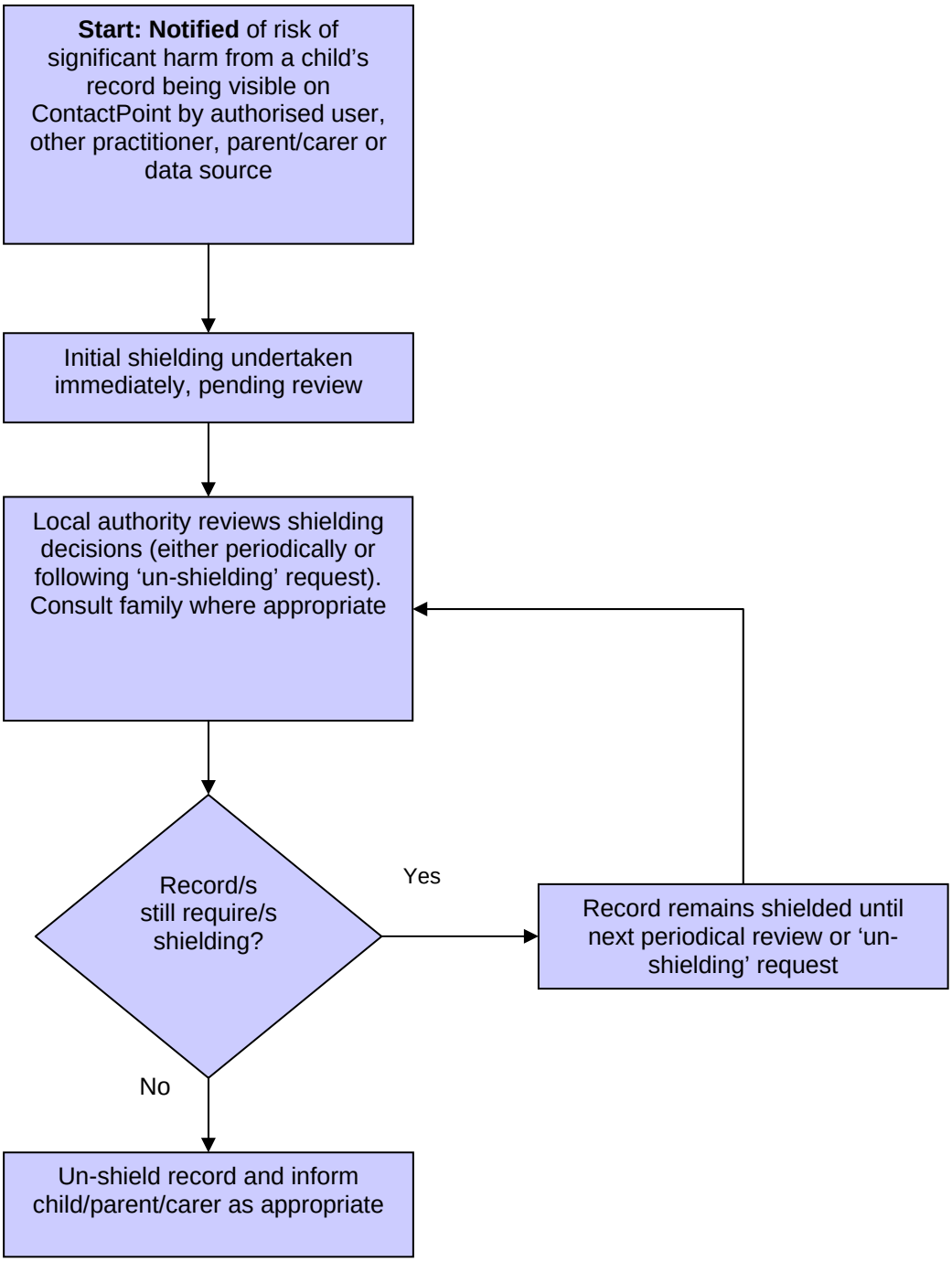
B10 Consent (Retaining a child record above 18 or Indicating 'Sensitive Services') (See 3.30 and 3.34-3.36)



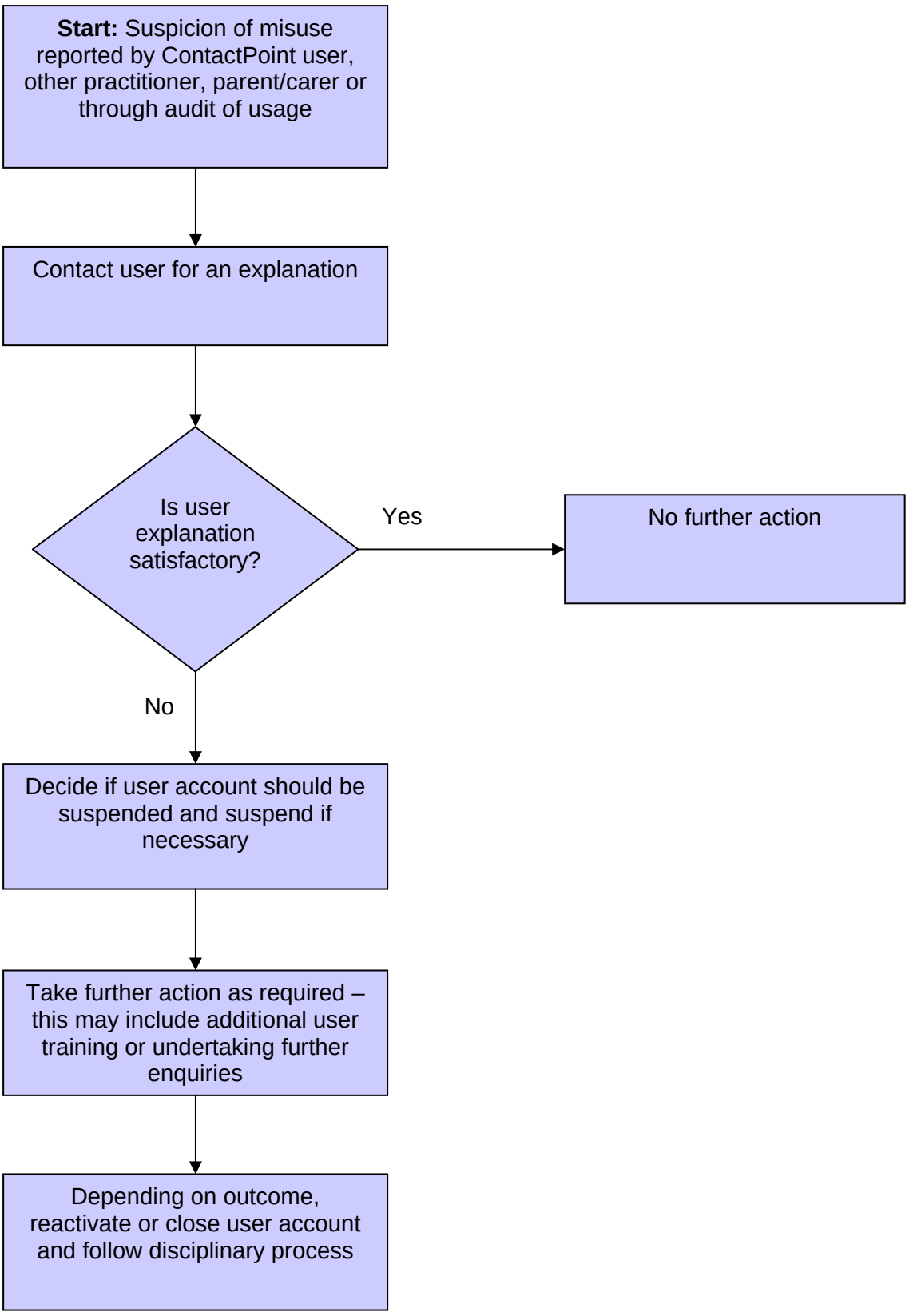
B11 Brokering Contact Between Users and 'Sensitive Services' (See 3.48-3.52)



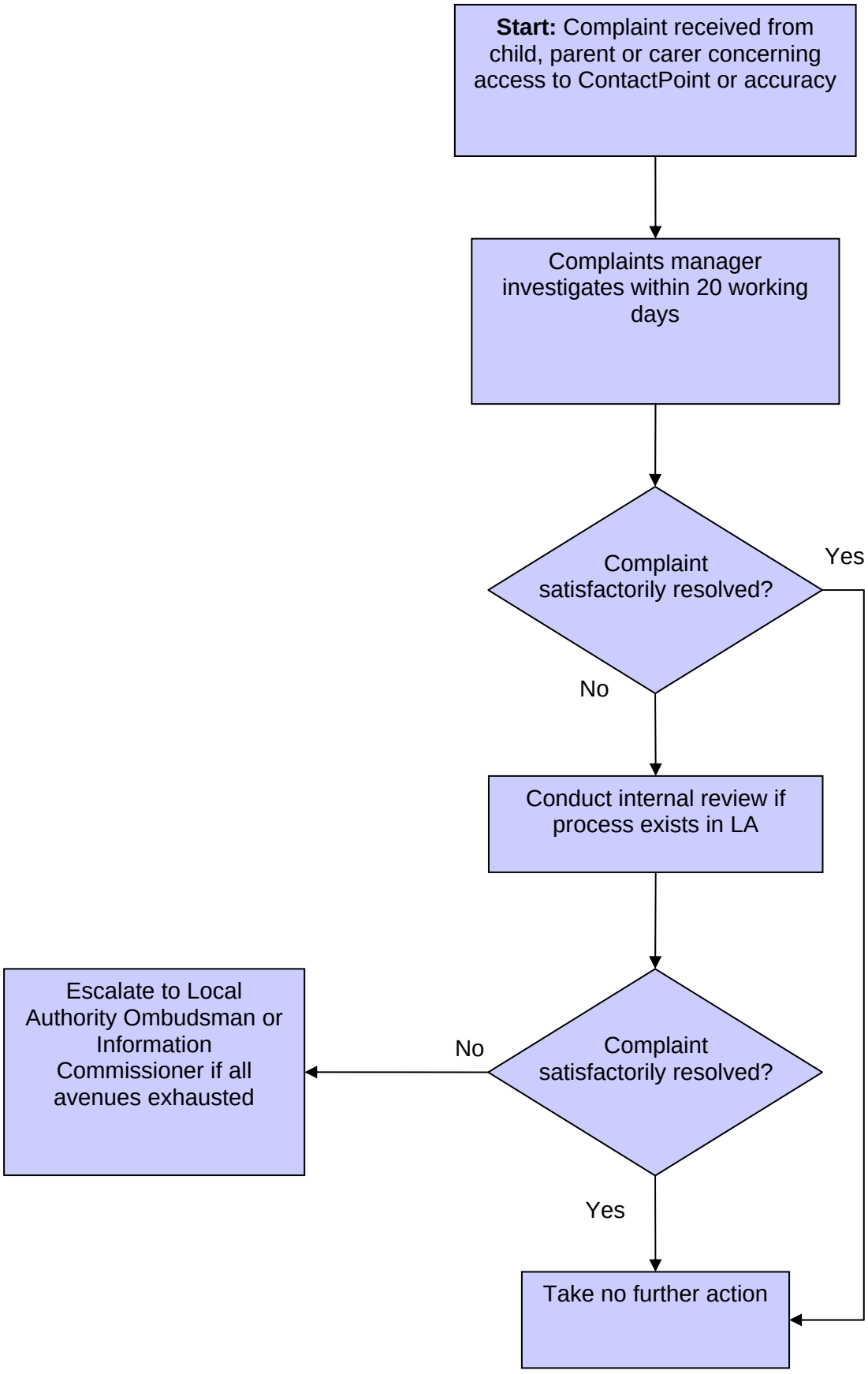
B12 Shielding Records (See 4.63 - 4.69)



B13 Managing Suspicious Usage See 3.9 - 3.12



B14 Complaints Procedure See 4.17-4.21



Annex C - GLOSSARY AND REFERENCE

Glossary of Terms Used

C1 **Best View -** This is where data from multiple sources is assembled by ContactPoint to form a single child record based on quality and reliability. The best view can allow for alternative names and addresses to be displayed.

C2 **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' prectitioners, extending the retention of records beyond 18 or making a SAR) 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. Implied consent is not sufficient for ContactPoint.

C3 **Data** 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 Data Protection Act 1998; or is none of the above but is recorded information held by a public authority.

C4 **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

C5 **Learning difficulties** – According to section 13(5) of the Learning and Skills Act (2000) an individual has learning difficulties if (a) they have significantly greater difficulty in learning than the majority of their peers or (b) they have a disability which prevents 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 he or she is or will be taught is different from that which has been spoken in his/her home at any time.

C6 **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.

C7 **Data Processor** - any person other than an employee of the data controller who processes the data on behalf of the data controller.

C8 **Data Subject -** an individual who is the subject of personal data.

C9 **Lead professional -** a practitioner who takes the lead to co-ordinate provision and be a single point of contact for a child and their family, when a range of services are involved with that child or family and an integrated response is required (see *The Lead Professional: Practitioner's Guide)*

C10 **Mediated access** is where an authorised ContactPoint user accesses ContactPoint through another authorised user.

C11 **Metadata** – identifying data which accompanies all data which is provided to ContactPoint. It includes the identity of the data source the time and date that data was provided to ContactPoint. 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.

C12 **Ordinarily Resident** – Although there is no general statutory definition of 'ordinary residence' it should usually be interpreted as referring to the place a person has voluntarily settled for the regular order of their life. 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.

C13 **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 C.22-C.24).

C14 **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 about children.

C15 **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 sent to your phone.

C16 **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.

C17 **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).

C18 **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. More often, significant harm is a compilation of significant events, both acute and longstanding, which interrupt, change or damage the child's physical and psychological development. Some children live in family and social circumstances where their health and development are neglected. For them, it is the corrosiveness of long-term emotional, physical or sexual abuse that causes impairment to the extent of constituting significant harm. In each case, it is necessary to consider any maltreatment alongside the family's strengths and supports (see *Working Together to Safeguard Children - Annex A*).

C19 **Subject Access Request (SAR)** is a request made under the Data Protection Act 1998 (DPA) by an individual to see information which is held about them by any organisation. The SAR is handled by the data controller, which in the case of the ContactPoint is the local authority responsible for a record.

C20 **Well-being** has a legal definition based on the five *Every Child Matters* outcomes; the achievement of these outcomes is in part dependent upon the effective work to safeguard and promote the welfare of children.

ContactPoint Reference

C21 **Information to be included on ContactPoint**

The records contain basic demographic details and contact details for the child, and name and contact details for their parents/carers. The basic demographic details of the child that are held are:

- name;
- address;
- gender;
- date of birth;
- a unique identifying number; and,

- where the person has died, the date of the person's death.

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 specialist/targeted services.

Contact details for those providing sensitive services (see C17) with informed and explicit consent will be indicated as an unspecified sensitive service involved. 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.

ContactPoint indicates whether an assessment using the Common Assessment Framework (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.

C22 Persons and bodies required to supply information to ContactPoint:

- Local authorities;
- Primary care trusts, acute care trusts, strategic health authorities and special health authorities;
- Police and British Transport Police authorities;
- Police forces including the British Transport Police;
- Local probation board;
- Youth offending team;
- Prisons, youth offending institutes and secure training centres;
- Any person providing services under section 114 of the Learning and Skills Act 2000 (Connexions);
- Learning and Skills Council;
- Maintained schools, FE institutions, special schools (including non-maintained special schools) and independent schools; and

C23 Persons and bodies permitted to supply information to ContactPoint:

- Government departments headed by a Secretary of State;
- Childcare providers (registered under part 3 of the Childcare Act 2006);
- Voluntary organisations which hold data on children in the area;
- Registered social landlords;
- 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; and,
- Children and Family Court Advisory Service (CAFCASS).

C24 **Persons authorised to use ContactPoint -** Access 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:

- Members of the local authority ContactPoint Management team;
- Anyone employed by, or contracted to provide services to, a local authority, who carries out functions under sections 10 and 11 of the Children Act 2004;
- Local authority social services staff (including children's home, residential family centre and foster care staff);
- Local authority 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;
- 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);
- Local authority 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.

To become authorised users, individuals must also meet certain further conditions which are established in regulations (see 2.7).

Further Sources of Reference

C25 **DfES**

Further information on ECM:CfC and ContactPoint is available on the ECM website: http://www.ecm.gov.uk/contactpoint/

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);

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/resources-and-practice

The *Common Core of Skills and Knowledge for the Children's Workforce* (DfES, 2005):
http://www.everychildmatters.gov.uk/deliveringservices/commoncore/

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/

Guidance on the Common Assessment Framework for children and young people (CAF):
http://www.everychildmatters.gov.uk/deliveringservices/caf/

Guidance on Lead Professional:
http://www.everychildmatters.gov.uk/deliveringservices/leadprofessional/

Sure Start Children's Centres Practice Guidance (DfES, 2005):
http://www.surestart.gov.uk/publications/

Adoption and Children Act Regulations 2003:
www.dfes.gov.uk/adoption/lawandguidance

C26 Information Commissioner's Office

The Data Protection Act 1998:
Subject Access Request:
www.ico.gov.uk/

C27 Department for Constitutional Affairs

Privacy and data-sharing: the way forward:
www.dca.gov.uk/foi/sharing/

C28 Department of Health

Confidentiality: NHS Code of Practice (DH, 2003):
www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

C29 General Medical Council

Confidentiality: protecting and providing information:
www.gmc-uk.org/guidance/library/confidentiality.asp

C30 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

C31 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 (Youth Justice Board, 2005):
www.youth-justice-board.gov.uk/Publications/Scripts/prodView.asp?idproduct=211&eP=PP