ContactPoint: Consultation on Draft Guidance

Consultation Response Form

The closing date for this consultation is: 27 July 2007
Your comments must reach us by that date.

department for
education and skills
creating opportunity, releasing potential, achieving excellence

The information you provide in your response will be subject to the Freedom of Information Act 2000 and Environmental Information Regulations, which allow public access to information held by the Department. This does not necessarily mean that your response can be made available to the public as there are exemptions relating to information provided in confidence and information to which the Data Protection Act 1998 applies. You may request confidentiality by ticking the box provided, but you should note that neither this, nor an automatically-generated e-mail confidentiality statement, will necessarily exclude the public right of access.

Please tick if you want us to keep your response confidential. ☐

Name	
Organisation (if applicable)	
Address:	

If your enquiry is related to the policy content of the consultation you can contact:

Nigel Dexter 0207 273 4857 (nigel.dexter@dfes.gsi.gov.uk)

or

Richard Mallinson 0207 273 5165 (richard.mallinson@dfes.gsi.gov.uk)

If you have a query relating to the consultation process you can contact the Consultation Unit on:

Telephone: 01928 794888

Fax: 01928 794 311

e-mail: consultation.unit@dfes.gsi.gov.uk

Please check one of the boxes that best describes you as a respondent:

☐ Child/young person	☐ Parent/carer	☐ Education – LA Staff
☐ Education – School/College Staff	☐ Health – PCT/SHA Staff	☐ Health – GP/Staff
☐ Social Services Staff	☐ Early years and childcare	☐ Local Authority
☐ ISA Team/Trailblazer	☐ Children's Trust	☐ Connexions service
☐ Youth justice and probation	☐ Police	☐ Voluntary and Community Sector
☐ Youth Services	☐ Representative bodies	☐ Other (please specify below)

Please Specify:

Introduction

This draft ContactPoint guidance is 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.

Section 12 requires that any person or body establishing or operating a database under section 12 of the Children Act 2004 must have regard to any guidance given to them by the Secretary of State. In addition, this guidance is for all those who will have access to ContactPoint (ContactPoint users) and their managers, bodies which supply data, and partner organisations.

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 a range of statutory duties relating to children. It will be the quick way for a practitioner to find out who else is working with the same child or young person, making it easier to deliver more coordinated support.

This consultation response form is made up of a number of paragraphs from the guidance document relating to each of the 12 questions asked by the consultation. The downloadable guidance and consultation documents contain colour-coded user boxes and flowcharts. The online system does not support this functionality, therefore it may be necessary to view or download the Word or PDF version of the Guidance, or the Flowchart PDF, when using the online response form.

Questions

Accuracy

Q1: Is the draft guidance sufficiently clear about the importance of accuracy?

Please use the comments box below to say how this can be made clearer:

☐ Yes ☐ No ☐ Not Sure

Comments:

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

- ensure the completeness and accuracy of the records for children ordinarily resident in their area

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 add data to ContactPoint, or to systems which supply data to ContactPoint, must fulfil their duties under the Data Protection Act 1998.

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.

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.

3.25 **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.

3.29 **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.

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.

4.1 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.

4.16 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.

4.47 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.

4.50 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.

Unauthorised Access and Misuse

Q2: Is the draft guidance sufficiently clear about how unauthorised access to ContactPoint and misuse will be managed?

Please use the comments box below to say how this can be made clearer:

☐ Yes	☐ No	☐ Not Sure

Comments:

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.

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[1] (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 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.

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

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

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.

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.

4.34 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.

4.43 **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.

Subject Access Requests

Q3: Is the draft guidance sufficiently clear about an individual's rights to see information held about them?

Please use the comments box below to say how this can be made clearer:

☐ Yes ☐ No ☐ Not Sure

Comments:

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.

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.

Complaints Procedure

Q4: Does the draft guidance sufficiently explain how local authorities are required to manage complaints relating to ContactPoint?

Please use the comments box below to say how this can be better covered:

☐ Yes ☐ No ☐ Not Sure

Comments:

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

- establish and maintain a complaints procedure in relation to the operation of ContactPoint in their area.

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).

Shielding

Q5: Is the draft guidance sufficiently clear about how the 'shielding' of child records will operate?

Please use the comments box below to say how this can be made clearer:

☐ Yes ☐ No ☐ Not Sure

Comments:

4.63 Shielding records

ContactPoint has the facility to hide from view or 'shield' data from ContactPoint users. 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.

It is important that where there is a real risk of significant harm or a serious crime, a child record is shielded without delay

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 un-shield 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.

Flowcharts (Annex B)

Q6: Are the flowcharts helpful in explaining processes within this guidance?

Please use the comments box below to expand on your answer or suggest further processes which may benefit from flowcharts:

☐ Yes ☐ No ☐ Not Sure

Comments:

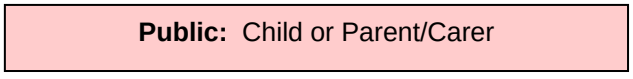
6. Flowcharts

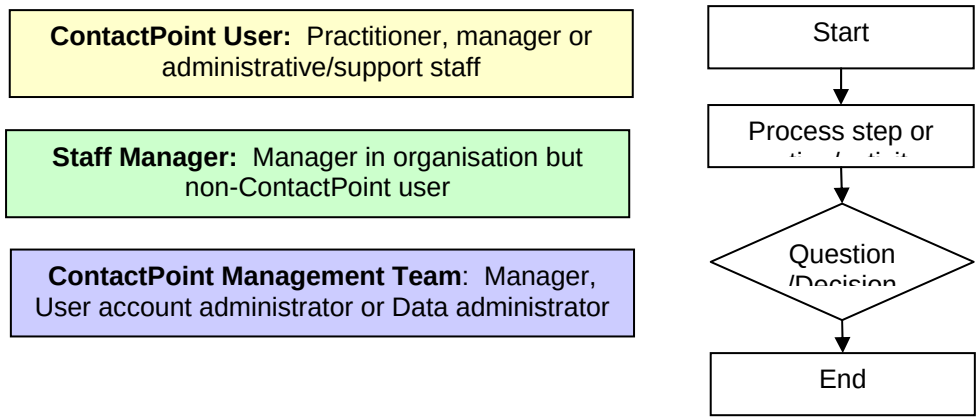
These flowcharts support a number of the processes covered in this guidance. They are intended as a guide and are not definitive. There may be established processes within your organisations which cover or can be adapted to cover or join up with these, which you may wish to follow.

- User Access - Direct (6.4)
- User Access - Mediated (6.5)
- Managing new ContactPoint Users (6.6)
- Manually requesting/creating a new child record (6.7)
- Consent- Retaining child records above 18 & Indicating 'Sensitive Services' involvement (6.8)
- Brokering Contact Between Users and 'Sensitive Services' (6.9)
- Subject Access Request by Young Person (6.10)
- Subject Access request on behalf of a Child/Young Person (6.11)
- Shielding Child Records (6.12)
- Managing Suspicious Usage (6.13)

6.1 Key

The flowcharts follow the colour-coding established in the table at 1.12, and used throughout, depicting actions by ContactPoint users and non-users. Actions are depicted by the shapes as shown below, right:





6.2 References are made between the relevant sections and flowcharts throughout the guidance. You may wish to view or download the Flowchart PDF to assist you when answering this question

6.3 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.

Paragraphs relating to the next four questions form the bulk of chapters 2, 3 and 4, some of which are used elsewhere within this document. To avoid repeating much of these, some paragraphs unique to each of these next questions have been included, together with lists of relevant paragraphs from the guidance itself. You may wish to view or download the guidance to assess the level of detail of these topics.

Contents & Purpose (Chapters 2, 3 & 4)

Q7: Does the draft guidance cover all the necessary topics to support the appropriate use of ContactPoint?

Please use the comments box below to say which other topics you would like to see covered:

☐ Yes ☐ No ☐ Not Sure

Comments:

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.

Contents

Local Authority responsibilities (Chapter 4 and '*ContactPoint Management Team*' boxes)

Q8: Is the draft guidance sufficiently clear about the statutory responsibilities of local authorities?

Please use the comments box below to say which topic(s) should made clearer:

☐ Yes ☐ No ☐ Not Sure

Comments:

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.

1.12

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	Responsible for maintaining data

	administrator	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

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)
- 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 In some partner organisations, a person designated by the Secretary of State will have responsibility for managing users within that organisation.

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:

5) **Coverage** – the number of children covered as a proportion of the total child population in England;
6) **Completeness** – the degree to which the full set of data required by ContactPoint is provided;
7) **Uniqueness** – the absence of duplicate child records within a data source; and,
8) **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.

Supporting Practitioners (Chapter 3 & 4.53-4.81)

Q9: Is the draft guidance sufficiently clear about how ContactPoint will support practitioners working with children?

Please use the comments box below to say which topic(s) should made clearer:

☐ Yes ☐ No ☐ Not Sure

Comments:

3. USING ContactPoint

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)

3.45 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.

4.

- Child moves between local authorities (4.53)
- Child leaves England (4.60)
- Shielding records (4.63)

Implementation

Q10: Do you foresee any challenges arising from implementing ContactPoint using this guidance?

Please use the comments box to let us know what you think these challenges might be and how they might be resolved:

☐ Yes ☐ No ☐ Not Sure

Comments:

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.

1.3 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 design

The design of ContactPoint will comprise of a centrally maintained national system with a record for each child[2] (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.

1.16 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.

Contents

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

User Groups

Q11: Is the use of colour-coded, user-specific, guidance helpful for readers? (Definitions of users can be found in the table at 1.13.below)

Please use the comments box below to identify users that you think should be covered by the guidance or if you feel the guidance could be formatted in a more helpful way:

☐ Yes ☐ No ☐ Not Sure

Comments:

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

General Comments

Q12: General Comments

We are keen to know your views and welcome any further general comments that you might have on this draft guidance; this can include the format, content and language used.

Comments:

Thank you for taking the time to let us have your views. We do not intend to acknowledge individual responses unless you place an 'X' in the box below.

Please acknowledge this reply ☐

Here at the Department for Education and Skills we carry out our research on many different topics and consultations. As your views are valuable to us, would it be alright if we were to contact you again from time to time either for research or to send through consultation documents?

☐ Yes ☐ No

All UK national public consultations are required to conform to the following standards:

1. Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.

2. Be clear about what your proposals are, who may be affected, what questions are being asked and the timescale for responses.

3. Ensure that your consultation is clear, concise and widely accessible.

4. Give feedback regarding the responses received and how the consultation process influenced the policy.

5. Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.

6. Ensure your consultation follows better regulation best practice, including carrying out a Regulatory Impact Assessment if appropriate.

Further information on the Code of Practice can be accessed through the Cabinet Office Website: http://www.cabinetoffice.gov.uk/regulation/consultation-guidance/content/introduction/index.asp

Thank you for taking time to respond to this consultation.

Completed questionnaires and other responses should be sent to the address shown below by **27 July 2007**

Send by post to:

ContactPoint Guidance Consultation
ContactPoint National Team
Westminster Suite
Caxton House
6-12 Tothill Street
London
SW1H 9NA

Send by e-mail to: ContactPointGuidance.consultation@dfes.gsi.gov.uk