



Contact Point Policy 2009

Table of Contents

| | |
|---|---------|
| 1. Introduction & Context | Page 3 |
| 2. Employee and Contractor Records | Page 4 |
| 3. Induction Process & Job Description | Page 4 |
| 4. Exit Policy | Page 4 |
| 5. eCRBs | Page 5 |
| 6. Training | Page 5 |
| 7. Misuse of ContactPoint & Security Breaches | Page 5 |
| 8. Internal Audit/Control | Page 6 |
| 9. Shielding | Page 7 |
| 10. Mediated Access | Page 8 |
| 11. Token Handling | Page 8 |
| 12. Ensuring Personal Data is Accurate | Page 9 |
| 13. Loss of Passwords | Page 9 |
| 14. Access to Records (SARs) | Page 9 |
| 15. Emergency Shielding Override | Page 10 |
| 16. Workstation Requirements | Page 10 |
| 17. Network Infrastructure | Page 11 |
| 18. First Line Support | Page 11 |
| 19. Handling Disputed Data | Page 12 |
| . | |

1. Introduction and context

ContactPoint is the quick and easy way for those working with children and young people to find out who else is working with the same child or young person, making it easier to deliver more coordinated support.

ContactPoint is part of the Every Child Matters programme to improve the lives of children and young people with a strong emphasis on early intervention for those who could benefit from additional services. It aims to help ensure all children get access to the services and support to which they are entitled - as well as safeguarding vulnerable children.

ContactPoint is designed to make it easier for those working with children and young people to do their jobs; free up a significant amount of time and reduce duplication of effort, enabling practitioners to spend more time delivering services.

Access to this basic online directory will be strictly limited to those who need it to do their job. All authorised users will have completed mandatory training, have security clearance (including enhanced Criminal Records Bureau clearance) and have a user name, a password, a PIN and a security token to access ContactPoint.

ContactPoint will contain basic identifying information about all children and young people in England up to their 18th birthday, and contact details for services working with them. ContactPoint will NOT contain any case information (such as case notes, assessments, medical records, exam results or subjective observations).

ContactPoint will not change any rules governing confidentiality or sharing information when practitioners discuss a child's needs. Everyone who works with children and young people should ensure that they follow established guidelines on information sharing and exercise professional judgement.

Section 12 of the Children Act 2004 provides the legislative basis for establishing ContactPoint. The primary purpose of ContactPoint is to support those practitioners working in children's services who are under the duties specified in Section 10 and Section 11 of the Children Act 2004 - the duty to cooperate to improve well-being, and the duty to safeguard and promote welfare of all children in England.

Following widespread consultation with stakeholders and Parliament, the Regulations - officially known as The Children Act 2004 Information Database (England) Regulations 2007 - came into force on 1 August 2007.

2. Employee and Contractor Records

Records are kept of employees and contractors as per Essex Schools Recruitment policy.

3. Induction Process & Job Description

Access to ContactPoint can only be gained after training has been received. We must keep records of staff that have been trained. This must be retained for 6 years following the date of employment termination or transfer to another post. If an employee has been trained to use ContactPoint in another post and wishes to transport their training, we must collect evidence of their training from either the previous employer or the local ContactPoint Team and document.

All new staff that will be using ContactPoint will undergo training provided by the ContactPoint Team before they can access the system. Courses will be available to book on-line. The course for the most suitable time will be booked by the School for the employee. An eCRB less than 3 years old needs to be in place before training is given. Records of staff training received will be kept within the staff personnel file.

The text below is included in the HR manager Job Description

This role encompasses the usage of the ContactPoint National Children's Database. To use ContactPoint you must have a current enhanced Criminal Records Bureau check (e-CRB) which is less than 3 years old and undertake the relevant training and security checks. ContactPoint will provide you with a security token which remains the property of the Local Authority, and must be kept secure at all times. When you cease employment in this role you must return the token to your Manager.

4. Exit Policy

When a ContactPoint User leaves their post we, their employer, must inform the ContactPoint Team at Essex County Council that their ContactPoint account should be suspended. Tokens are non-transferable. The employee must return the ContactPoint token to us, their employer. It is our responsibility to return the token by registered post to Essex County Council at the following address:

ContactPoint Team
Schools, Children and Families Directorate
PO Box 47
County Hall, E2
Chelmsford
Essex CM2 6WN

ContactPoint tokens remain at all times the property of Essex County Council.

We must ensure the leaver is aware that to continue to access ContactPoint once they have left their employment with us is misuse of the ContactPoint system and they are potentially committing a criminal offence under the Computer Misuse Act 1990.

5. eCRBs – Enhanced Criminal Records Bureau

ContactPoint requires ALL users to be eCRB (less than 3 years old) checked, to undergo standard ContactPoint user training and to be issued with tokens and passwords before any access is granted to the ContactPoint system. Records must be kept of all ContactPoint users, detailing the pre-conditions required for access to ContactPoint, the date of their training, and any subsequent joiners, movers or leavers within the school. Records must be kept for 6 years after the leave date of the employee.

The appropriate person HR Manager within Alec Hunter Humanities College will need to ensure ContactPoint users do not lapse their eCRB and that they are renewed within 3 years. These records must be maintained for 6 years after the employee has left our employment. Any employee with an elapsed eCRB will be suspended as a User until their eCRB is renewed, or their account will be closed and the token must be returned to the Local Authority.

Any employee who fails their eCRB check will have their use of ContactPoint withdrawn. The school must inform the Local Authority ContactPoint Team immediately and return the token issued to the employee by the Local Authority.

6. Training

Access to ContactPoint can only be gained after training has been received. We must keep records of staff that have been trained, which must be retained for 6 years following the date of employment termination or transfer to another post. If an employee has been trained to use ContactPoint in another post and wishes to transport their training, we must collect evidence of their training from either the previous employer or the local ContactPoint Team and document.

7. Misuse of ContactPoint & Security Breaches

The security of all systems, including ContactPoint, is the responsibility of all employees. If you suspect someone is misusing the system you must report this incident. You must report ALL breaches of security to your Manager, or if not appropriate to the Head of the school. Support must be given to staff wishing to report incidents outside the normal reporting procedures. All instances of security breaches must be logged detailing actions taken.

Any misuse of the ContactPoint system will lead to appropriate sanctions. These can include, if appropriate, fines or imprisonment under the provision of the Data

Protection Act 1998 and Computer Misuse Act 1990 and permanent deletion of the User account.

Through the active audit trail ContactPoint's usage is monitored and checked daily. This is verified both locally by the Local Authority and nationally by the Department of Children, Schools and Families (DCSF). Any misuse will be communicated to the Manager of our school who will follow our investigatory and where appropriate, disciplinary procedure to deal with the incident referring where appropriate to the Code of Conduct, Confidentiality (section 5) and Disciplinary (Misconduct) Policies of Essex County Council. The user account will be suspended during investigation. Records of any investigation must be held for 6 years after the conclusion of the case.

The list below sets out a number of activities that are strictly forbidden when accessing ContactPoint, and is not exhaustive.

- access to and operating on information or systems to which you are not authorised, commonly called 'hacking';
- any use of ContactPoint for personal gratification, gain or malicious intent;
- accessing child records of family members, colleagues' friends or neighbours unless a professional relationship exists to provide services;
- using another user's account or credentials to gain access to ContactPoint;
- use of any techniques to bypass monitoring and/or auditing on the system; overwhelming ContactPoint with requests (outside the operational limits of the system) such that it will cause the system to be inaccessible to others (known as a 'denial of service attack');
- divulging of any information obtained from ContactPoint to an unauthorised third party;
- any act that contravenes ContactPoint policies or applicable legislation;
- bypassing any formal process for the provision of information when acting as a mediator;
- wilfully altering records such that it will negatively impact on the integrity of the information held on the system;
- any act of vandalism to the computer system or data e.g. the introduction of malicious software, and bypassing of any security controls to gain access to ContactPoint or related system resources.

8. Internal Audit/Control

The school is required to ensure that the accreditation profile is regularly maintained and monitored to ensure there is minimal risk of a security breach that may lead to damage to the organisation's and/or ContactPoint's reputation.

Staff usage must be monitored to ensure that policies and procedures are being adhered too referring where appropriate to the Essex County Council Schools Human Resources model Audit Policy Document.

9. Shielding

Essex County Council will control shielding activity on ContactPoint for those children residing in Essex during the ContactPoint roll-out period. Any practitioner or parent/carer can request a shield be placed on a child's record by completing the Shield Request Form available at:

<http://www.essexcc.gov.uk/vip8/ecc/ECCWebsite/dis/guc.jsp?channelOid=14181&guideOid=126194&guideContentOid=129778>

The Deputy Head teacher Students and Staff will make the decision to shield a Child record on ContactPoint if they believe that should the Child record remain unshielded it may place the Child at risk of significant harm. The Children Act 1989 introduced the concept of significant harm as the threshold that justifies compulsory intervention in family life in the best interests of children. Shielding is principally intended to prevent the whereabouts of a Child being identified either through:

Visibility of their address details from ContactPoint,
or;
ContactPoint providing enough information for a likely whereabouts to be deduced (e.g. a service involvement address).

The need for shielding could arise for example where:

- a Child/Young Person is adopted where there is little or no contact with birth parent(s) or wider family members;
- a Child/Young Person and/or their Parent/Carer, are fleeing abuse or domestic violence; and/or;
- a Child/Young Person and/or their Parent/Carer or family member are subject to Police protection.

If a ContactPoint User believes that the Child's whereabouts should be closely guarded in order to protect the Child from a known and valid threat, they should either:

- Locate the Child record on ContactPoint and 'shield' manually. We must notify the Local Authority ContactPoint Team that we have done so.

Or, if we do not have appropriate access rights:

Immediately inform the Local Authority ContactPoint Team using the Shield Request Form that the record needs to be shielded.

All shielded records will be reviewed by the Local Authority at regular intervals. When the authorised personnel in this organisation believe the shielding is no longer appropriate they should:

Upload a new Child record without the Shielded Record Notification;

Or, if we do not have appropriate access rights;

Inform the Local Authority ContactPoint Team that the record can have the shielding removed.

You should also consider the safeguarding of family members and/or co-resident Children/Young People as the records for these individuals may also need to be shielded.

10. Mediated Access

If we are unable to connect to ContactPoint through our own technology, it is possible to request a 'mediated' service through the Local Authority. To use this service we must be in possession of all our secure log-in information to enable the session.

Mediation should not be confused with information Sharing. Mediation is the use of a Third Party to obtain information from ContactPoint about a child. Information Sharing is asking the Third Party to share information which they hold.

When we access mediated services we must keep our own record of the interaction. As with all ContactPoint use, mediated sessions will be audited. It is essential that we have confirmation that our session has ended.

The process for this function is the use of a log book to record the date, time and mediator of mediated sessions undertaken on ContactPoint by the Deputy Head teacher Students and Staff.

11. Token Handling

ContactPoint tokens will ONLY be issued to employees who have successfully completed their ContactPoint training. These tokens can ONLY be used to access the ContactPoint system.

ContactPoint tokens remain at all times the property of Essex County Council. Tokens will be issued at the training sessions for ContactPoint Users and we will log the token number issued to each staff member in our training records.

IMPORTANT

NEVER share your security token with others.

Keep your security token with you, or locked up, at all times.

If you lose your token, or are aware that someone else may have used your token, you must immediately inform your Local Authority ContactPoint Team who, subject to security checks, will issue a new token.

12. Ensuring Personal Data is Accurate

A duty is placed on the holders of personal data by the Data Protection Act 1998. Subject to section 27(1), it shall be the duty of a Data Controller to comply with the data protection principles in relation to all personal data with respect to which he is the Data Controller. Breaching the Data Protection Act principle that 'Personal information must be accurate and up to date' may result in a financial penalty.

We will regularly check with parent/carers that their child's details are accurately recorded on our system by reminding them each term in our Herald Newsletter and website

It is each Practitioner's responsibility to ensure that all children with whom they have 'first contact' are searched for on ContactPoint to facilitate high levels of data accuracy. Contact details should be checked each time we meet with the Child or Parent/Carer. Processes must be put in place to ensure that data quality is maintained in respect of all records, even those kept for a required one year after the end of Practitioner involvement.

Any changes of Child data should be made to our Case Management System and not ContactPoint.

Staff with ContactPoint accounts are required to keep their personal data on ContactPoint up to date. Passwords should be changed as required. Security questions must be set up to allow for identification where a password is not available.

Users will be provided with training regarding the correct and incorrect usage of ContactPoint.

13. Loss of Passwords

If a ContactPoint User loses their password they must contact the Local Authority ContactPoint User Administration Team who, subject to security checks, will issue a new password. Failure to keep your password and security token secure may result in suspension or closure of your ContactPoint account.

14. Access to Records (SARs)

Subject access requests (SAR)

Individuals have the right to request access to any personal data an organisation which controls the data holds about them (Section 7 of the Data Protection Act 1998). This is known as a 'subject access request' (SAR). In the case of information held in a ContactPoint record, Local Authorities will take the lead in responding to local SARs made in relation to ContactPoint. A SAR can only be made by or on behalf of the individual to whom the personal data relates and must be made in writing. It may specifically refer to ContactPoint or may be a

broader request which can include ContactPoint data. The address for SAR enquiries is:

ContactPoint Team
Access to Records
Schools, Children & Families
Essex County Council
PO Box 47
County Hall
Chelmsford
Essex CM2 6WN

Local authorities have established procedures for handling SARs (for other purposes). These procedures should be followed for requests relating to information held on ContactPoint. SARs will be responded to within 40 days. There is an identity verification process to ensure that the requestor has a legal right to view the data held. The Data Protection Act contains a number of exemptions where such personal data should not be released - these should also be considered when deciding whether to disclose details from ContactPoint. Care must be taken to ensure that this process is not abused by an estranged parent trying to track down a child.

15. Emergency Shielding Override

Limited Users with appropriate access rights will be able to access the Emergency Shielding Override. This will give a 'one time only' view of a shielded record. All requests must be explicit and confirmation will be required. All overrides will be investigated by the Local Authority ContactPoint Team on the next working day. Misuse of the system will result in fines or imprisonment under the provision of the Data Protection Act 1998, the Children Act 2004 and the Computer Misuse Act 1990. We will be required to investigate such instances and report back to the Local Authority within 24 hours.

Those using the emergency shielding override are likely to be those who come into contact with children during unsociable hours - such as Police Officers or Social Services Duty Workers where gaining access to information held in ContactPoint may help inform their decision about the appropriate action to take in the absence of other Practitioners to talk to.

16. Workstation Requirements

All workstations used for ContactPoint must be an approved and maintained build supplied by the organisation. The operating system and security-related software must be actively supported and security patches promptly applied. The workstation must either have installed (or be in the environment that adequately provides) firewall, anti-virus and anti-spyware facilities. These must be configured by our school and users must not circumnavigate them. Any breaches must be

investigated by us and brought to the attention of the local ContactPoint Manager.

Workstations must not be left unattended when logged onto ContactPoint unless they have been securely locked so long as the workstation is not in a public area. The workstation screen must not be easily readable by anyone other than the logged-in user. In open plan areas a screen should be used, and a sign such as 'restricted access' used to emphasise the need for privacy.

17. Network Infrastructure

All access to ContactPoint uses HTTPS on the standard TCP port 443, with a minimum of 128 bit symmetric key length. Client-side certificates are not used.

Case Management System (CMS) Access

Where access to ContactPoint is through a Global Service Institute (GSI) network workstations must connect to the network via a case management system (CMS) that has been modified to perform Simple Object Access Protocol (SOAP) calls to the ContactPoint core.

Web Access

ContactPoint has been configured to use only known IP addresses or address blocks that are dedicated to the workstation or organisation network. ContactPoint is designed to prevent the use of temporary IP addresses. A user's workstation can access the ContactPoint web interface via a Virtual Private Network (VPN); however you can access the web interface directly. Separate authorisation lists will be maintained for web and SOAP interfaces.

Any upgrades or changes to our CMS, whether modified or otherwise, must be notified to the local ContactPoint Data Manager.

18. First Line Support

The school will provide first line support to its users. Our support facility will be advertised to all ContactPoint users within our school and processes will be in place to track and monitor service requests through to completion. Our first line support staff will contact, where appropriate, a ContactPoint expert who will assist in resolving any issues. Staff are advised that they should use their normal support routes and not go directly to the ContactPoint Team.

19. Handling Disputed Data

Data held by our school may be disputed by the Child or Parent/Carer. If data we have provided to ContactPoint has been disputed, and it is not clear whether the data is actually incorrect, this needs to be shown on ContactPoint to avoid any risk of being in breach of the Data Protection Act 1998.

If the data exists on ContactPoint and it is not appropriate for it to be changed to the Child or Parent/Carer's satisfaction on our case management system (and

hence transmitted to ContactPoint), we will contact the ContactPoint Team at our Local Authority, who will mark the data in ContactPoint as 'disputed'.

Where a Local Authority has been notified of disputed data it will be sent to us for investigation. If consistently poor data is supplied, we will be de-accredited to ContactPoint as a data source.

Any requests to change the legal name of a child on our system must be supported by provision of legal documents authorising the change of name. Without sight of these documents we are unable to amend the legal name but are able to show the desired name as a 'known as' name.

Declaration

I confirm that the information in this document is accurate and that the processes are in place to support ContactPoint use within this school.

Signed

(Headteacher).....

Chair of Governors.....

Date.....

This document is issued by

Essex County Council, Schools, Children and Families Directorate.

You can contact us in the following ways:

By Post:

ContactPoint Team, Schools, Children and Families Directorate
Essex County Council, PO Box 297, County Hall, Chelmsford, CM1
1YS

By telephone:

0845 603 7639

By fax:

01245 493403

By email:

ContactPoint@essex.gov.uk

Visit our website:

www.essex.gov.uk

www.everychildmatters.gov.uk

The Children's Trust Approach www.ctaessex.org.uk

The information contained in this document can be translated and/or made available in alternative formats, on request.

Published May 2009.



Essex County Council