**Child Sexual Exploitation and Missing from Home/Care:**

**North West Cross-Border Information Sharing Protocol**

1. **Introduction**

All Local Safeguarding Children Boards (LSCBs) have developed multi-agency, coordinated responses to identifying children and young people who may be at risk of Child Sexual Exploitation (CSE) and/or are at risk because they go missing from their home or placement. These include localised systems for sharing information on risks relating to individual children/young people and of development ‘trigger’ and protection plans.

1. **Background**

LSCBs acknowledge there are challenges associated with CSE and children who go missing, where cross-border characteristics of risk, including trafficking, are a consideration. Such scenarios include where children/young people:

* attend school in a local authority other than that in which they are ordinarily resident;
* are transported/travel to another local authority area for social, leisure or other reasons;
* are Looked After and placed in another local authority, including where the placement out of area/at a distance is intended to reduce risks associated with CSE, gang association and other factors;
* are trafficked across borders.
1. **Purpose**

Whilstthere are good examples of how local authorities/LSCBs work together across boundaries to share information to protect children, there is scope to further improve and embed information sharing, particularly across police service areas. Specifically, information sharing relating to CSE and Missing from Home (MFH)/Care can, via the provisions of this protocol, be improved in order to:

* ensure children/young people at risk of CSE/Missing are safeguarded and their welfare promoted;
* enable appropriate intelligence to be shared to prevent harm to others (including in respect of known ‘hotspots’ or where CSE risks are associated with particular institutions or locations); and
* facilitate the prevention or detection of crime and/or capture or prosecution of offenders.
1. **Implementation**

**This is not an operational emergency response contact – if there are immediate concerns about a child this would need to be referred in the usual way**

By agreeing to be party to this protocol, local authorities must:

* Consult and comply with local information governance requirements in relation to processing and storing information.
* Identify a Single Point of Contact (SPOC) for providing, accepting and handling notifications.
* Make notifications to SPOCs in other areas solely in line with the stated purpose of this protocol.
* **Only provide information by means of encrypted documents shared via secure e-mail**.
* Ensure, via the SPOC, information is shared with relevant individuals in the receiving local authority area to ensure that the child is safeguarded and intelligence is used effectively to prevent harm to others.
* Include adequate, accurate and relevant information including screening tools identifying risk, ‘flagging’ information, trigger plans for intervention and protection and contact details for the home local authority.
* Only share information where there is a direct link between the child/young person and the local authority area where there are identified risk factors to them or others.
* Ensure those making, accepting or processing notifications understand individual agency information governance rules and actively consult with Information Governance lead/ Caldicott Guardian as relevant.
* Fulfil responsibilities for applying relevant exemptions of the Data Protection Act 1998 on a case-by-case basis where notifications are made in relation to the prevention or detection of crime and/or capture or prosecution of offenders.
* Acknowledge receipt of notifications to the ‘home’ local authority SPOC by whom the notification was made. The SPOC at the receiving local authority should also inform the home local authority of how the information has been processed and any action taken.
* Inform the SPOC at the receiving local authority where the home local authority has identified risk has reduced or been removed.
* Follow local information governance procedures on the retention of information, including review and destruction processes.
1. **Review**

A system for formal and ongoing review will be established to identify good practice and propose changes to this protocol. A formal review will be completed **not later than 30 October 2016**

1. **Related resources**



**Appendix A**

**Contact Arrangements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Local Authority** | **Single Point Of Contact** **(**This is not an operational referral process and **must be a secure email address)** | **Named lead and contact** ( if applicable) | **Web link to reporting procedures** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Appendix B**

**Principles**

The principles underpinning this protocol are based upon consideration of published advice of the Office of the Information Commissioner (ICO) in relation to the Data Protection Act 1998 and non-statutory Department for Education advice [*Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers*](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf) *March 2015*.

The Data Protection Act recognises that it is sometimes appropriate to disclose personal data for certain purposes to do with criminal justice or the taxation system. In these cases, individuals’ rights may occasionally need to be restricted. In particular, the Act deals with several situations in which personal data is processed for the following “crime and taxation purposes”:

* the prevention or detection of crime;
* the capture or prosecution of offenders;

Detailed guidance is provided in the ICO publication [*Using the crime and taxation exemptions*](https://ico.org.uk/media/1594/section-29.pdf)which summarises responsibilities as follows:

* The crime and taxation exemptions are based on the purpose for which the personal data is being processed, not on the type of organisation doing the processing. The purposes relevant to this exemption are the prevention and detection of crime, the apprehension or prosecution of offenders, and the assessment or collection of tax.
* Data controllers do not have to fulfil their obligations to tell individuals how their data is being processed or respond to a subject access request (SAR), if doing so would prejudice the crime prevention and taxation purposes.
* Data controllers can disclose personal data without applying the usual data protection principles, if the disclosure is necessary for the crime prevention and taxation purposes.
* It is the data controller making the disclosure who is responsible for deciding whether the exemption applies in each case.
* The exemptions must be applied on a case by case basis, and should be used only when it is necessary to do so.

Practitioners should consider the ‘7 golden rules’ in sharing information under this protocol.

1. **Necessary and proportionate** - consider how much information you need to release. Any information shared must be proportionate to the need and level of risk. Consideration should be given to sharing plans for intervention and protection, including contact details for key professionals in the home local authority. Examples of approaches to this include the Phoenix ‘Trigger Plan’ shared amongst agencies in Greater Manchester. This is appended at the foot of this protocol.
2. **Relevant** - Only information that is relevant to the purposes should be shared with those who need it. Information should only be shared if there is a direct link for the child/young person and the local authority area where there are identified risk factors to them or others. This provision should ensure that there is no ‘blanket’ approach to sharing sensitive personal information on a police service area basis or other wider spatial level than is necessary.
3. **Adequate -** Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon. Information shared should draw upon a robust evidence base such as completed screening tools or risk assessment and be shared where a cross border risk exists for an individual child/young person.
4. **Accurate** - Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.
5. **Timely** - Information should be shared in a timely fashion to reduce the risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it. This protocol is intended to protect children and young people through reducing risk of harm, it is not an ‘operational contact’ process and does not replace existing mechanisms for notification and response to immediate safeguarding concerns.
6. **Secure** - information should be shared in an appropriate, secure way. Practitioners must always follow their organisation’s policy on security for handling personal information. Parties to this protocol retain organisational responsibilities to share, retain and use information in line with their own policies. **Any information shared across boundaries should only be sent within encrypted documents via secure e-mail addresses.**
7. **Record** - Information sharing decisions should be recorded, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. In line with each organisation’s own retention policy, the information should not be kept any longer than is necessary.