Lincolnshire Police
Information Sharing Agreement



# Information Sharing Agreement (ISA) betweenLincolnshire County Council Children’s ServicesandLincolnshire Police

Version: 8.0

(Revised – 24th February 25)

## Summary Sheet

**Reference number**: LP001/CS - Lincolnshire County Council Children’s Services

**Purpose**

This Information Sharing Agreement (ISA) defines the arrangements for the regular or volume sharing of personal information between the named partners.

The information shared will include personal data, special category data and criminal offence data.

This agreement will determine the named partners’ responsibilities in relation to relevant legislation including, but not limited to, Data Protection Legislation. It assists to enable partners to ensure that the sharing of information is justified, shared lawfully and securely.

**Partners (data controllers) to the agreement**

It is important to recognise that the recipient organisation will become the Data Controller for any personal information that is shared with them for the purpose/s described within this ISA.

* Lincolnshire Police, PO Box 999, Lincoln, LN5 7PH
* Lincolnshire County Council Children’s Services, County Offices, Newland, Lincoln, LN1 1YL

**Date Agreement comes into force:** 01st September 2007

**Date of Agreement Review:** Six months after coming into force, then annually

**Agreement Owner:** Lincolnshire Police

**Agreement drawn up by**: Det. Supt Guy Collings, Lincolnshire Police

**Location of Signed Agreement**: Information Management Unit, Force HQ

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version No.** | **Date** | **Amendments Made** | **Authorisation** |
| 00/01 |  |  | DCI Harris |
| 00/02 |  | Appendix A - Request for information FormAppendix B - Enquiry to Establish If Child is Subject to a Child Protection Plan | DCI Harris |
| 2.0 |  | Updated at annual review | Mr D Massey - ISA Officer |
| 3.0 |  | Updated due to changes requested by D/Supt Guy Collings | Sally Wood/ D/Supt Collings |
| 3.1 |  | Updated following the incorporation of changes suggested during consultation | D/Supt Collings |
| 4.0 | 24 Oct 12 | Paras 5.5, 8.1, 9.2, 9.4 and Appendix A amended | E D Tedder - IS Officer |
| 5.0 | 11 June 13 | DA Processes specifically 4.11 and 5.6Removed Appendix B - Enquiry to Establish If Child is Subject to a Child Protection Plan and references to this form – no longer used by PPU CRU or CSinserted 5.7 and 5.8  | S NorburnL Chapman – IS Officer |
| 6.0 | 14 Jan 1522 Apr 1522 May 154 Sept 154 Oct 16 | Para 2.4 added.Section 7 & 10 amended.Amendments made after consultation with C Hammond (CRU D/Inspector) (S Mumford (RRD Supervisor) & S Norburn (Domestic Abuse Co-ordinator).Appendix A updated.Appendix B added - Lincolnshire Children’s Services and Lincolnshire Police Protocol on Managing Domestic Abuse Notifications & Referrals where Children are involved/resident in the Household.Section 5.4 amended after consultation with partner agency and C Hammond (CRU D/Inspector)Data Protection Officer replaced RRD SupervisorData Protection /FOI Manager replaced RRD Manager Disclosure of Police Information Form replaced P698B Form.Appendix B updated (15/08/2016) | L Chapman – IS OfficerL Chapman – IS OfficerL Chapman – IS Officer |
| 7.0 | 28 Dec 172 Oct 1829 Jun 2015 Jul 20 | Appendix A – amended.Revised template adopted due to enactment of the DPA/ UK GDPR 2018Appendix A – amended to Appendix 3Appendix B – amended to Appendix 4Revised template adopted.Amendments made after consultation with the force Lincolnshire Partnership Safeguarding Hub Inspector and the Domestic Abuse Coordinator. | L Chapman – IS OfficerL Chapman – IS OfficerL Chapman – IS OfficerL Chapman – IS Officer |
| 8.0 | 5 Sept 2326 Apr 2413 Jan 2520 Jan 2524 Feb 25 | Annual Review – Section 3 amended to include a list of the types of information the police may share.Appendix 4 Amended to include revised Children’s Services Request Form. Appendix 5 Amended to include revised Protocol on Managing Domestic Abuse Notifications & Referrals where Children are involved/resident in the Household.General updates for job titles and department name changes. Update on new request form.Revised Children’s Services Request Form added (Appendix 4)Removed all reference to DBS checks. Added DPO SPoC. | L Chapman – IS OfficerD Stenner – IS OfficerSally Wood – IMU ManagerDonna Stenner - IS OfficerDonna Stenner - IS Officer |

## 1. Introduction and Purpose

###  Introduction

1.1 Lincolnshire Police are committed to partnership working, and continually look for opportunities to work more closely with local identified partners to detect, prevent and reduce crime and anti-social behaviour.

1.2 In adopting this partnership approach it is important that the policies/practices of the agencies involved complement each other to ensure that any action taken is appropriate, necessary, proportionate and consistently applied.

1.3 This agreement has been produced with the obligations of the statutory guidance, the “Management of Police Information” (MoPI) in mind. APP information Management, “MoPI sharing” provides standards that must be applied by the Chief Constable when sharing information with external agencies. This Information Sharing Agreement (ISA) is compliant with such standards.

### 1.4 Purpose

 The purpose of this agreement is to enable information to be disclosed to Lincolnshire County Council Children’s Services during child protection and child in need enquiries, including those within cases of domestic abuse.

 It will incorporate measures aimed at:

* Facilitating a coordinated approach to child protection and child in need enquiries.
* Facilitating the collection and exchange of relevant information;
* The pursuit of criminal or civil proceedings in relevant cases, either by Lincolnshire Police or Lincolnshire County Council Children’s Services.
* Ensuring that the sharing of information meets one or more of the policing purposes.

## 2. Specific Purpose

### 2.1 Aims and Objectives

 The aim of this agreement is to support Lincolnshire Police and Lincolnshire County Council, Children’s Services to work together and share personal data to enable both organisations to effectively safeguard, support and improve the lives of children within Lincolnshire.

### 2.2 Context of the Processing

 Information will be requested by Children’s Services in the following circumstances:

* When Children’s Services are undertaking a child in need assessment (section 17) and/or completing a protection/ care plan;
* In relation to a Section 47 investigation;
* In relation to an emergency or planned placement assessment for a child with a family member or friend.
* When completing an investigation under the LSCP allegations Policy.

 The information shared through this agreement will fulfil the purpose of the agreement, by ensuring that Children’s Services have all the relevant information they require in order to safeguard, protect and improve the lives of Children in Lincolnshire.

## 3. Types of Information to be Shared

3.1 **Lincolnshire police may share:**

* Relevant PNC (Police National Computer) prints.
* Relevant information relating to convictions and cautions associated with violent offences, sexual offences, drug related offences, harassment offences, public order offences and domestic related offences.
* Relevant information relating to allegations associated with violence, drugs, harassment, sexual abuse, public order and domestic abuse.
* Relevant information relating to incidents associated with violence, drugs, harassment, sexual abuse, public order and domestic abuse.
* Relevant information relating to child protection issues.
* Safeguarding information including domestic abuse, substance abuse, concerns for safety, and mental health occurrences.

 Disclosed information may include the following details:

* A brief description of the incident, together with the Modus operandi (MO);
* Relevant court dates;
* Outcome of the incident, i.e. caution, NFA (No Further Action), conviction details etc.
* Relevant bail conditions
* Relevant restraining order details.

 This is not an exhaustive list; further information may be provided if it is deemed relevant and proportionate to the request.

3.2  **Request criteria and police department responsibilities:**

Via the use of a Lincolnshire County Council Children’s Services Request Form, (see appendix 4) Lincolnshire County Council Children’s Services will submit a request to Lincolnshire Police. The form will either be submitted to the Lincolnshire Partnership Safeguarding Hub within the Protecting Vulnerable Persons Unit (LPSH) or the Partner Agency Disclosure Officer (PADO) team within the Information Management Unit (IMU)

 **LPSH requests**

* Requests for information should be submitted to the LPSH in the following circumstances:
* When a child protection referral is made and a Section 47 joint investigation has begun, e.g. through a strategy discussion/meeting or child protection conference. In these instances, application for disclosure of information will be made through the LPSH.
* When Lincolnshire County Council Children’s Services are carrying out an investigation under Section 47.
* When Lincolnshire County Council Children’s Services are carrying out an initial assessment in order to inform the decision as to whether the Section 47 threshold is reached.
* When Lincolnshire County Council are making an immediate (same day) placement of a child or for the purposes of urgent safety planning to identify safe adults.

 **PADO – IMU requests**

 Requests for information should be submitted to the PADO team - IMU in the following circumstances:

* When Lincolnshire County Council Children’s Services are carrying out a child in need assessment under Section 17.
* When the request relates to a child subject or previously subject to a child protection plan.
* When Lincolnshire County Council Children’s Services are faced with the immediate need to place a child, but this is not a same day request.
* Where children may be victims or witnesses to domestic abuse and therefore at risk of harm.
* Where allegations are made against individuals who work with children.
* Adults who may have harmed/pose a risk to a child but don't work with children

3.2.1 The following areas of business which may be checked by the Police in response to such a request are:

* PNC (Inc. Firearms Revocation)
* Niche
* PND

3.3 **Lincolnshire County Council Children’s Services may share:**

* Details of referrals made to the Local Authority Designated Officer (LADO) concerning allegations made about people who work with children.
* Information gathered as part of a section 47 investigation with relevant agencies and the child/young person and/or their family or any party acting on their behalf at a child in need meeting / child protection conference to assist in safeguarding the child through a multi-agency plan unless there are specific reasons why information cannot be shared in the presence of the family this includes information disclosed by the police. Note that it is the responsibility of the social worker to have sought disclosure in advance of a child protection conference. Police representatives at this forum will NOT be used as a means of seeking initial disclosure, instead their role in respect of disclosure will be limited to providing an update to information already provided.

3.4 Partners to this agreement must ensure that the information shared is the minimum amount of information required to achieve the purpose. Therefore, disclosures will contain factual information only, using the principle that **“the minimum disclosure required is the maximum disclosure permitted.”**

3.5 In respect of any child protection issue or concern, there may be a need to disclose information which relates to doubts and suspicion.

3.6 In respect of allegations made against individuals who work with children, there may be a need to disclose information, which relates to previous criminal enquiries, convictions and police intelligence.

3.7 Section 47 Children’s Act 1989 allows Children’s Services to request information from other agencies as part of an ongoing child protection enquiry. It should be understood that a failure to disclose information which could prevent a tragedy, can also result in criticism but above all could result in a child being harmed.

3.8 Information must only be shared on a ‘need to know’ basis.

## 4. The Sharing Process

4.1 All requests for information MUST be made in writing using the Lincolnshire County Council Children’s Services Request Form (copy at appendix 4). Without this form, ALL applications (except in urgent cases, see 4.8) will be rejected and returned. The request form (Appendix 4) is utilised for the following reasons:

* + It records the request for information and the necessity to do so.
	+ It provides evidence of consultation between the Police and Lincolnshire County Council Children’s Services in relation to a referral about a child in need.
	+ It assists to record the decision-making process where a child is suspected to be suffering, or likely to suffer, significant harm and Section 47 Children Act enquiries are required to be undertaken.

4.2 Requests and replies to requests must be made via a secure encrypted e-mail system. Where the partner does not have access to a secure encrypted e-mail system, the information must be encrypted via some other means, such as Windows password encryption, and the password sent via other means, such as telephone.

4.3 Forms must be completed electronically; endorsement of Children’s Services staff must be completed prior to emailing to IMU/LPSH.

4.4 Disclosure must be made within 10 working days, from receipt of the request except in urgent cases (see 4.8). **Lincolnshire County Council Children’s Services staff are encouraged to apply at the earliest opportunity. Requests for such information from PVP staff either locally or at conference will not be accepted.**

4.5 The Data Protection Supervisor in the Information Management Unit (IMU) will be consulted in respect of each instance where information is to be disclosed and will undertake the decision-making role and record same; except in cases involving a Section 47 Joint Agency Investigation, where the D/Sgt in the Lincolnshire Partnership Safeguarding Hub will carry out this function.

4.6 In the initial stages of a child protection or child in need referral, it can be difficult to determine a course of action or whether a single or multi agency enquiry will result. Information may be disclosed on receipt of a referral or during a strategy discussion or meeting by LPSH staff. However, all information disclosed by either the PADO team or the LPSH must be recorded on the NICHE occurrence on the OEL under the header DISCLOSURE, this will also be added to the disclosure form which will be attached to the NICHE occurrence, a copy of which will be sent to Lincolnshire County Council Children’s Services along with the information being disclosed. In either case a copy of the form will be retained in the respective unit and a record made on NICHE stating what has been disclosed and why. **Following any strategy discussion/consultation with the LPSH, it is the specific responsibility of Lincolnshire County Council Children’s Services to submit a copy of the SOS Strategy Discussion recording form, which must be forwarded within 10 days to LPSH for recording onto NICHE. Failure to submit the competed SOS Strategy Discussion form will result in a lack of continuity and a breakdown in information flow.**

4.7 To ensure that the obligations under the Data Protection Act 2018, UK GDPR and Human Rights Act 1998 are fulfilled the following procedure will apply:

* The Children’s Services form will be submitted via email to the Partner Agency Disclosure Officer, who will review the request and determine whether the request will be met and what checks will be undertaken. If the request meets the relevant criteria the request will be logged and processed on niche.
* In the case of a Section 47 Joint Investigation a SOS Strategy Discussion Form will need to be submitted to the LPSH, who will review the request and determine whether the request will be met and what checks will be undertaken and record same.

4.8 There will be instances whereby urgent action is required on behalf of either/both of Lincolnshire Police and Lincolnshire County Council Children’s Services to prevent an immediate risk to a child. In such cases information that would normally be subject of a written request by Lincolnshire County Council Children’s Services can be shared verbally by the Lincolnshire Partnership Safeguarding Hub. Lincolnshire County Council Children’s Services will send a written Children’s’ Services request form (appendix 4) confirming this request on the same day of the initial information sharing and LPSH will provide written confirmation of disclosure given. LPSH staff will make an entry on the NICHE system to record the fact that verbal disclosure has taken place.

4.9 **Domestic Abuse Incidents where children are present or reside at the address.** Information will be shared by LPSH direct to Lincolnshire County Council Children’s Services. A full protocol document is available detailing the process agreed between the two agencies (see Appendix 5).

4.10 Disclosures completed by email must be done via a secure/encrypted messaging system. If you are unsure as to whether an e-mail address you have been provided is secure, you can check the recipient’s email by using the following link: <https://www.checktls.com/>

 If you are unsure whether the email address provided is safe, you should contact your security representative. For Lincolnshire police this will be the Vetting and Security Manager.

4.11 Disclosed information must be recorded on the Disclosure of Police Information Form and returned to the applicant. A copy will be filed and logged on NICHE.

### 4.12 Ad Hoc Requests

 Requests for ad hoc information, for example, requests from a partner not named within this agreement but for the same purpose of the agreement, will be directed to the SPoC and dealt with on a case-by–case basis. Ad hoc requests should be completed in line with the disclosing partner’s current policies and procedures.

### 4.13 Responsibilities

**4.13.1 Lincolnshire County Council Children’s Services**

* That all requests for information meet the criteria outlined.
* That the information disclosed by Lincolnshire Police is stored securely in accordance with the Data Protection Act 2018 & UK GDPR.
* That inaccuracies in the information provided by Lincolnshire Police are promptly notified to the Data Protection Supervisor or LPSH officer.

**4.13.2 Head of IMU and LPSH Inspector**

* Supporting staff to share information appropriately and within service level agreement (SLA) timescales.
* Providing a system for recording decisions on whether to disclose or not disclose.
* Ensuring that the process of disclosing information is adhered to by both those in a supervisory and user capacity.

**4.13.3 Data Protection Supervisor and LPSH Sergeant**

* Supporting staff to disclose information appropriately and within service level agreement (SLA) timescales.
* Auditing on an ad hoc basis, the decision to disclose made by users, including the necessity, accuracy and adequacy of information disclosed.
* Checking whether the decision to disclose meets a policing need as laid out in this document or other legal duty or power.
* Ensuring that information disclosed does not compromise any Police operation or the safety of others.
* Ensuring that a risk assessment process (contained within the Disclosure of Police Information Form) is adhered to by the user when making a decision to disclose information. Providing feedback to staff on their performance.

**4.13.4 Users PADO and LPSH Staff**

* Ensuring that information is relevant, accurate and adequate for the purpose for which it is being disclosed.
* Ensuring that when personal information is disclosed, the requirements of the Data Protection Act 2018 & UK GDPR and the common law duty of confidence have been fulfilled.
* Recording any decision to disclose or not to disclose **on the Disclosure of Police Information Form and NICHE.**
* Checking whether the decision to disclose meets a policing need as laid out in this document or other legal duty or power.
* Ensuring that information disclosed does not compromise any Police operation or the safety of others.

## 5. Roles and Responsibilities Under this Agreement

### 5.1 Single Points of Contacts (SPoC)

 Each Partner must identify a Single Point of Contact (SPoC) who will be responsible for the implementation of this agreement. The SPoC should be notified of any disputes or breaches to the agreement. The SPoC details are provided in the table outlined below:

 **Police SPoC (PADO – IMU)**Title: Data Protection Supervisor
Contact Details: 01522 212428

 **Police SPoC (LPSH)**
Title: LPSH Sgt
Contact Details: 01522 212365

 **Lincolnshire County Council Children’s Services SPoC**
Title: Head of Service – Safeguarding Children’s Services
Contact Details: 01522554739 / Jo.casey@lincolnshire.gov.uk

 **Information Sharing Officer**Contact details: isa@lincs.police.uk

 The Police SPoC will work alongside the Information Sharing Officer who will jointly be responsible for the development of this agreement. The Information Sharing Officer will be responsible for instigating the review process and will work in conjunction with all named SPoCs in relation to updates and amendments to the ISA.

 **Data Protection Officers (DPO)**

 Each Partner must appoint a Data Protection Officer to undertake the statutory responsibilities set out in Articles 37-39 of the UK GDPR and Sections 67-71 of the Data Protection Act 2018. In addition to the SPoCs, the DPOs should also be notified of any disputes or breaches to this agreement. The contact details for the DPOs are listed below:

 **Lincolnshire Police:**

Name: Jennifer Johnson

Title: Head of IMU (Information Sharing Unit)

Contact: jennifer.johnson@lincs.police.uk

**Lincolnshire County Council:**

Name: Amy Jaines

Title: Information Governance Manager (DPO)

Contact: dpo@lincolnshire.gov.uk / 01522 555029

5.2 All SPoCs have a responsibility to ensure that an audit trail of the information sharing is maintained and made available when required. Any changes in SPoC details will be notified as soon as practicable.

5.3 In order for Lincolnshire Police to share information, the Single Point of Contact (SPoC) or staff making the disclosure must ensure that information is shared in line with the Policing Purposes as set out in the Management of Police Information Code of Practice. In line with the section 39A of the Police Act 1996, Chief Officers are required to give “due regard” to this statutory code. The Policing Purposes are described as:

* Protecting life and property;
* Preserving order;
* Preventing the commission of offences;
* Bringing offender to justice, and
* Any duty or responsibility arising from common or statute law.

 The disclosures should also be made in conjunction with the Law Enforcement purposes. Law Enforcement Purposes are defined in Section 31 DPA 2018 as:

1. Prevention, investigation, detection or prosecution of criminal offences
2. Execution of criminal penalties
3. Safeguarding against and preventing threats to public security.

### 5.4 Conflict of Interest

 The Signatory and/ or Single Point of Contact (SPoC) has a responsibility to ensure that staff members responsible for requesting and disclosing information from or to Lincolnshire Police are not affiliated with a group/ organisation that may result in a potential conflict of interest. For example, if a staff member is affiliated with the British National Party or a vigilante group this would indicate a conflict of interest; therefore it would not be appropriate to share police information. Such competing interests can make it difficult to fulfil his or her duties impartially. A conflict of interest exists even if no unethical or improper act results.

## 6. Compliance with the DPA/UK GDPR Principles

6.1 Partners to this agreement must ensure that the process of information sharing is completed in accordance with the Data Protection Act 2018 (DPA 2018) and /or the UK GDPR. In particular, the six principles of either the DPA 2018 or the UK GDPR will need to be adhered to depending on whether processing relates to law enforcement processing or general processing. The Data Protection principles are listed in section 35 – section 40 of the DPA 2018 and the UK GDPR principles are listed in Article 5(1) of the UK GDPR (See Appendix 2 for further information). This agreement will demonstrate how the sharing of information complies with the principles of the DPA or the UK GDPR.

### 6.2 Principle 1/(a) – Lawfulness, fairness and transparency (if applicable)

#### 6.2.1 Lawful Basis for information Sharing

 For the purpose of this agreement, the sharing of personal information is between the Police and a Non-Competent Authority, and the sharing of personal data is for Law Enforcement Processing and non-Law Enforcement Processing, therefore the following lawful basis apply for the processing of personal information.

####  Law Enforcement Processing – Lincolnshire Police

 **Competent Authorities**

 Lincolnshire Police are a Competent Authority, their investigatory and enforcement powers are derived from numerous Acts which include but are not limited to the following; the Police and Criminal Evidence Act 1984 (PACE), the Criminal Procedures and Investigation Act 1996, the Serious Organised Crime and Police Act 2005.

 **Schedule 8 – Processing Sensitive Data Under Part 3 of the Data Protection Act (DPA) 2018**

 In order to share sensitive data, in relation to law enforcement purposes the processing must meet at least one of the conditions in Schedule 8 of the DPA. In relation to this processing, the following Schedule 8 conditions are satisfied:

 1. the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.

 3. to protect the vital interests of the data subject or of another individual.

 4. to protect an individual from neglect or physical, mental or emotional harm, or protect the physical, mental or emotional well-being of an individual aged under 18, or aged 18 or over and at risk, where consent cannot be given, and it is in the public interest.

 6. the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

 Lincolnshire Police have an appropriate policy document in place. The policy document outlines the conditions for processing special category and/ or criminal offence data and how the organisation ensures compliance with the principles.

 **Transferring sensitive personal data from Part 3 to Part 2**: Personal data, including Special Category Personal Data collected under DPA 2018 Sections 29-31 for the law enforcement purpose will only be transferred from DPA 2018 Part 3 into DPA 2018 Part 2 processing as special category personal data where a condition in DPA 2018 Schedule 8 is met. The data will then be processed as special category data where the requirements and conditions are met as set out in the paragraphs outlined below:

####  Sharing Personal Information for Non-Law Enforcement Purposes

 In order to share Personal Data for non-law enforcement purposes you must satisfy a condition from Article 6, Chapter 2 from the UK GDPR. The processing of personal data relating to this agreement satisfies the following condition(s):

* UK General Data Protection Regulation (UK GDPR), Chapter 2, Article 6 (‘Lawfulness of processing’ conditions):
* (c) Legal obligation: the processing is necessary for compliance with a legal obligation to which the data controller is subject;
* (d) processing is necessary in order to protect the vital interests of the data subject or another natural person;
* (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Information sharing which relates to special category data is strictly prohibited unless it satisfies at least one of the additional lawful bases set out in Article 9 (i.e. conditions for the ‘Processing of special categories of personal data’) of the UK GDPR. In relation to this agreement, the following lawful bases for processing special category data have been identified:

* UK General Data Protection Regulation (UK GDPR), Chapter 2, Article 9:
* (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
* (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In addition to the selection of (g) above, the processing needs to meet a specific substantial public interest condition set out in Schedule 1 of the Data Protection Act 2018. In relation to this agreement the processing satisfies the following conditions from Schedule 1 Part 2, DPA:

10. Preventing or detecting unlawful acts

11. Protecting the public

18. Safeguarding of children and individuals at risk

 Criminal Conviction and Offence data: Article 10 UK GDPR

 Processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

 In order to share information in relation to Criminal data for non-law enforcement purposes Lincolnshire Police must ensure that they comply with UK GDPR article 10 and a condition from DPA Schedule 1, Part 1 or Part 2 or Part 3. In relation to this agreement the processing complies with the following condition(s):

 10. Preventing or detecting unlawful acts

 11. Protecting the public

 18. Safeguarding of children and individuals at risk

 30. Protecting individuals’ vital interests.

#### Legal Powers to share Personal information with the Police

 Partners to this agreement may share personal information with Lincolnshire Police provided that they have a lawful basis to do so, and the purpose is compatible with the purpose for which the information was originally collected (Principles 1 and 2).

 Disclosure from the general processing of one partner necessary to meet the law enforcement purpose of the other will occur by virtue of:

 Article 6(1)(e) - Public Task where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

 Article 9(2)(g) – Substantial Public Interest by virtue of the DPA (2018) and the following substantial public interest conditions from Schedule 1 apply:

 Part 2 (10). Preventing or detecting unlawful acts

 Part 2 (11). Protecting the public

 Part 2 (18). Safeguarding of children and individuals at risk

 Part 3 (30). Protecting individuals’ vital interests.

 Partners to this agreement will share personal information with the police when they are completing activities that do not fall within the remit of the law enforcement purposes. However, the activities will assist the Police to discharge the policing purposes referenced within this agreement. Therefore, the sharing of information as part of this agreement is compatible with the purpose for which the personal information was originally collected.

#### Legislation which requires consideration prior to the disclosure of information

* The Civil Evidence Act 1995;
* The Crime and Disorder Act 1998 (section 115);
* Common Law Powers of Disclosure;
* The Rehabilitation of Offenders Act 1974;
* The Human Rights Act 1998 (article 8);
* The Data Protection Act 2018;
* UK General Data Protection Regulation (UK GDPR) 2021;
* Court Orders;
* Children’s Act 1989;
* Working Together to Safeguard Children 2018 (last updated 2022)

#### 6.2.2 Fair and Transparent

 In order to comply with the principles of the DPA/ UK GDPR the processing must be fair to the data subject; therefore all partners must process personal information in ways which the data subject would reasonably expect. However, there are certain exemptions to the fairness and transparency aspect of principle (a) which may be utilised in order to support the purpose of this agreement. In order to assist with this agreement, information may be shared that has a negative impact on the data subject which may not be fair and transparent. However the adverse impact can be justified on the grounds of:

* Public safety
* Prevention of disorder or crime
* Protection of rights and freedoms of others
* the disclosure is required by law or in connection with legal proceedings

 Where an exemption does not apply, partners should provide individuals with concise, accurate and easy to understand information about how their personal information will be used in relation to the purpose.

 In order to support transparency named partner have a Privacy Notice in place which is available on the partners respective websites.

 This Information Sharing Agreement will be made publicly available on the force website.

### 6.3 Principle 2/(b) – Purpose Limitation. - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

6.3.1 Partners to this agreement will ensure that information shared for the purpose of this agreement will only be used for the specific purpose for which it was shared.

 The information must not be processed further in a manner that is incompatible with the purpose(s) of this agreement.

 Therefore, partners undertake to ensure that any reuse of shared data is lawful, compliant with the data protection principles and processed using appropriate safeguards to the rights and freedoms of the data subject.

### 6.4 Principle 3/(c) - Data minimisation (adequate, relevant and not excessive)

6.4.1 The sharing of personal information requires careful judgement to ensure that the data shared is relevant; therefore partners need to determine the necessity and proportionality of the disclosure. In relation to this agreement, it is believed that the information is both necessary and proportionate due to the following criteria:

 **Necessary:**

 The necessity to share information between the Police and Lincolnshire County Council Children’s Services is to provide information for risk assessment purposes to ensure effective safeguarding strategies are adopted either on an individual or community basis.

 It is important to note that this agreement has been formulated to facilitate the exchange of information between partners. Therefore, it is incumbent on all partners to recognise that any information must be justified on the merits of each case.

 **Proportionate**: It is proportionate to share the information as it is deemed that the identified purpose justifies infringing the data subject’s right to privacy and appropriate measures to meet the purpose are both fair and rational.

### 6.5 Principle 4/(d) – Accuracy – Personal data must be accurate and where necessary, kept up to date

6.5.1 It is the responsibility of all partners to ensure that the information they disclose is of sufficient quality for its intended purpose, bearing in mind the accuracy, validity, reliability, timeliness, relevancy and completeness. Reference should be made to the nature of the source and the information itself.

6.5.2 Prior to disclosing information, staff will ensure that to the best of their knowledge the information is accurate and up to date.

6.5.3 Partners must take reasonable steps to inform each other if they become aware that they have sent or received inaccurate data. Queries in relation to accuracy issues should be directed to the named SPoC in order to rectify or amend inaccurate data.

### 6.6 Principle 5/(e) – Storage limitation - Personal data must be kept for no longer than is necessary

6.6.1 The recipient of the information is required to keep it securely stored and when it is no longer required for the purpose for which it was requested, will safely dispose of it. In order to ensure compliance with the Data Protection Act, data should be kept no longer than is necessary, retention periods may vary between organisations. In accordance, with the Management of Police Information (MoPI) and the Limitations Act [1980] Lincolnshire Police will retain copies of the requests and responses for 6 years.

6.6.2 The original police data source will be deleted when it is no longer useful for a policing purpose, this will be done in line with Lincolnshire Polices Review, Retention and Disposal policies which are governed by MoPI guidelines.

6.6.3 Files containing information from partner sources will be reviewed in line with force policy.

6.6.4 Partner agencies should retain and destroy the shared information in accordance with statutory guidelines and internal policies. If no statutory guidance exists for the retention and deletion of data, information should be held in accordance with the fourth (d) and fifth principle (e) of the DPA/ UK GDPR.

### 6.7 Principle 6/(f) - Integrity and Confidentiality (Security) - Personal data must be processed in a manner that ensures appropriate security

6.7.1 In order to ensure the security of the shared data, it is important for partners to this agreement to establish common security measures. For the purpose of this agreement Appendix 3 sets out security guidance that should be adhered to. In addition, all partners should have relevant security policies in place which outline how they comply with the data protection principles regarding security. Partners should be at liberty to request a copy if deemed necessary.

#### 6.7.2 Information Breaches

 Breaches to the data protection legislation should be dealt with by the relevant partner’s policies and procedures and may need to be reported to the Information Commissioner’s Office (ICO).

 All agencies are reminded of the Data Protection Act/ UK GDPR Principles and Part 6, Section 170 (unlawful obtaining) and Part 7, Section 198 (liability of directors) Offences of the DPA 2018.

 It is the responsibility of all partners to notify the other party of any known breach or infringement immediately and remedial action must be agreed and actioned by all relevant agencies concerned.

 Security incidents should be reported immediately to the affected partner via the named SPoC who will report it to the appropriate person within their organisation.

## 7. Common Law of Confidentiality & the Human Rights Act

### 7.1 Duty of Confidentiality

 This Agreement takes into account the Common Law duty of confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified.

* Where disclosure is necessary to safeguard the individual, or others, or is in the public interest.
* Where there is a legal duty to do so.

### 7.2 The Human Rights Act 1998

 Under Section 8(1) of the Human Rights Act 1998, all data subjects have a right to a private family life and can be interfered with if justified and proportionate.

In relation to this agreement interference with this right may be justified because the processing is necessary and in the interest of:

* Discharging the common law police duties
* Preventing/detecting unlawful acts
* Safeguarding children and adults at risk

**8. Rights of the Data Subject**

### 8.1 Individuals’ rights

 Data protection legislation gives individuals certain rights over their personal information.

 The lawful basis for processing information and the exemptions available will determine which rights are available to the data subject. In relation to this agreement the following rights may apply:

* The right to access personal data held about them.
* The right to withdraw consent.
* The right to request that inaccurate data is rectified, and incomplete data is completed.
* The right to request restriction of processing.
* The right to object to decisions made on the basis of automated processing and/or profiling.

8.2 Partners are responsible for ensuring they have policies and procedures in place to support the individuals’ (data subjects’) rights listed above.

8.3 Partners to this agreement will determine whether an exemption to the data subject’s rights may apply, this will be considered on a case-by-case basis.

8.4 Enquiries relating to the data subject’s right, should be directed to the relevant partners’ data protection or information governance teams using the following details:

 Lincolnshire Police – dataprotection@lincs.police.uk

 Lincolnshire County Council Children’s Services

 CustomerInformationService@lincolnshire.gov.uk

## 9. Complaints, Breaches and Disputes

### 9.1 Complaints

 Complaints from data subjects, or their representatives, regarding disclosures made in relation to this agreement will be investigated first by the organisation receiving the complaint. Where necessary, the partner receiving the complaint may consult with other parties to this agreement, who will give reasonable assistance.

### 9.2 Breaches of the Terms of the Agreement

 Suspected breaches to the terms of this agreement should be referred to the partner responsible for drawing up the agreement. This will allow the responsible partner to determine whether a breach to the agreement has occurred and apply any remedial action or adjustments to the terms of the ISA as necessary.

 Major breaches may result in this agreement being temporarily suspended or withdrawn completely.

9.3 Any disclosure of information by an employee, which is done in bad faith or for motives of personal gain, will be the subject of an investigation and be treated as a serious matter. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents.

### 9.4 Disputes

 In the event of any dispute or difference arising between the partners due to this agreement, the Single Points of Contact shall meet in an effort to resolve the dispute or difference in good faith.

### 9.5 Termination and Amendments to the Agreement

 All partners may terminate the agreement at any time. They must inform all the Single Points of Contact, who in turn will inform the relevant staff within their Information Governance/ management team.

9.6 Any party may make suggestions for amendments to the agreement at any time.

**10. Freedom of Information Act 2000**

### 10.1 Freedom of Information Act 2000 (FOI)

 If a party receives a request for information under the Freedom of Information Act (FOIA) [2000] that relates to data that has been disclosed for the purposes of this ISA, it is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption under the provisions of the FOIA and to identify any perceived harms. However, the decision to release data under the FOIA is the responsibility of the agency that received the request.

**11. Review of the Information Sharing Agreement**

### 11.1 Review of the Information Sharing Agreement

 This ISA will be reviewed if there are any changes to the information sharing process, legislative changes, a new partner is added or in the event of a security incident.

11.2 In any case this Information Sharing Agreement will be reviewed six months after its implementation and annually thereafter. Any amendments to the agreement will be verified and signed off by all partners.

## 12. Signature

12.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purposes of this agreement.

12.2 Signatories must also ensure that they comply with all relevant legislation.

12.3 It is the responsibility of all signatories to ensure that:

* Realistic expectations prevail from the outset.
* Professional, ethical standards are maintained.
* The Data Protection Principles are upheld.
* The information exchanged is kept secure and confidentiality is maintained as appropriate to the information’s level of protective marking as defined by the Data Controller.
* A mechanism exists by which the flow of information can be controlled.
* Appropriate staff training is provided on this agreement.
* Adequate arrangements exist to test adherence to the agreement.

12.4 Parties to this Agreement are aware that the deliberate or reckless disclosure of personal data (obtained under this Agreement) to other organisations or person may amount to a criminal offence under the Data Protection Act 2018.

 **Signed on behalf of Lincolnshire Police:**

 Sign here: Kam Mistry

 Name: Kam Mistry

 Rank/Position: D/Supt Head of PVP

 Date: 20th January 2025

 **Signed on behalf of Lincolnshire County Council Children’s Services**

 Sign here: 

 Name: Tara Jones

 Rank/Position: Assistant Director, Children’s Services

 Date: 24th February 2025

## Appendix 1 - Glossary of terms and definitions

1. Controller - A person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of processing of personal data.

2. Criminal Offence data – Criminal Offence Data is personal data relating to criminal convictions and offences or related security measures and includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018 S11 (2))

3. Data Protection legislation – in relation to this agreement means the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

4. Data Subject – the individual who can be identified from the data.

5. Originating organisation – the expression “originating organisation” refers to the organisation that is disclosing personal information to the recipient organisation.

6. Personal Data – ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

7. Personal Information – the expression “personal information” may relate to personal data, special category data and criminal offence and conviction data.

8. Recipient organisation – the expression “recipient organisation” refers to the organisation that is in receipt of personal information from the originating organisation.

9. Sensitive processing (defined in DPA Part 3, Chapter 2 (35) (8)) –

1. the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
2. the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
3. the processing of data concerning health;
4. the processing of data concerning an individual’s sex life or sexual orientation.

10. Special Category data – Special category data included data revealing or concerning the following types of data:

* Racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership
* biometric data (when used for identification purposes);
* health;
* sex life; and
* sexual orientation

11. Wef – With effect from

## Appendix 2 – Data Protection Principles

* Law Enforcement Processing (LEP) - Part 3 Chapter 2 Section 35 – 40 DPA 2018; &
* General Processing - Article 5(1) of the UK General Data Protection Regulation (UK GDPR)/Part 2 DPA 2018

### LEP (Section 35-40):

#### Principle 1

The processing of personal data for any of the law enforcement purposes must be lawful and fair.

#### Principle 2

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

#### Principle 3

Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

#### Principle 4

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

#### Principle 5

The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

#### Principle 6

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

### General processing – Article 5(1):

#### Principle (a)

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’)

#### Principle (b)

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’)

#### Principle (c)

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)

#### Principle (d)

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)

#### Principle (e)

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’)

#### Principle (f)

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

## Appendix 3 - Lincolnshire Police Security Requirements

### Security Guidance

It is essential that the participating agencies provide personal or other sensitive information only to specific individuals authorised to receive it. The transfer, use, storage and retention of the information by each participating agency must comply with the Data Protection Act 2018 and should comply with the security requirements stipulated within this agreement. Any additional security requirements that an agency wishes to specify must be done so in agreement with all parties involved within this document.

### General Principles

Ensuring that personal information is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access is the sixth principle of the Data Protection Act 2018. Partners should ensure they have appropriate security in place and arrangements to monitor these.

A key issue, especially for electronic documentation, is the consistent use of encryption and secure information exchange. Unguarded exchange of personal information may not only infringe the rights of the individual subject or others that may be identifiable from the information, but also compromise the organisations sharing information or jeopardise any proceedings or legal measure based upon that information.

With remote working there is an issue about storing personalised information on flash drives/memory sticks and of encryption. Partners sharing personal information are responsible for ensuring laptops, drive or removable electronic media containing personal information used for remote working are encrypted and have Home Office approved levels of security. To comply with national guidance encryption should be at least 256 bit.

Recent Home Office guidance with respect to third party suppliers suggests that:

* 1. No unencrypted laptops or drives or removable electronic media containing personal information should be taken outside office premises.
	2. No transferring of any protected personal information from Home Office approved systems to third party suppliers owned laptops, PCs, USB keys, external drives and any other electronic media is permitted.

### Secure Information Exchange

Electronic exchange can be the most secure and auditable means of exchanging information provided this is done using suitable secure technology. Personal information should only be exchanged electronically using a secure messaging system.

Attendees at meetings where personal data is discussed must also ensure that controls applied to agenda and minute documents are as secure as those used for requesting and securing personal information, since these will often name the individuals being considered and contain elements of the information contributory to the decision-making process. Records of meetings and personal information must be subject to the principles set out in the ISA, particularly in relation to purpose and retention.

If a recipient organisation wishes to remove shared information from their premises, they must ensure that the information is kept secure at all times, must not be made available to individuals who are not authorised to see it, and must only be used for the purposes specified within the ‘Information Sharing Agreement’.

### Sharing information securely

It is important that information is shared securely. Those who receive personal data should take appropriate measures to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing. This includes when data is being shared and stored both electronically and manually (e.g. paper).

All designated Officers who have access to personal data should have been assessed for reliability in line with the employer’s requirements for the role, for example Disclosure and Barring Scheme (DBS) checks. A greater degree of staff vetting and/or training is needed where there is a greater importance that relevant data be secure.

The information Commissioner has issued the following guidelines concerning obligations for agencies:

1. Does the data controller have a security policy setting out management commitment to information security within the organisation?
2. Is the responsibility for the organisations security policy clearly placed on a particular person or department?
3. Are sufficient resources and facilities made availability to enable that responsibility to be fulfilled?

Shared information should be stored securely, and if no statutory guidance dictates otherwise, the recipient organisation should destroy the information when it is no longer needed for the purpose for which it was provided. If an organisation does not have the means to securely destroy shared information, they should consider returning the data to the originating organisation for destruction.

### Government Security Classifications

All Lincolnshire Police information is classified in line with the Government Security Classifications (GSC). In order to ensure that the same protection is afforded to Lincolnshire Police data once it has been disclosed to a partner agency, the partner organisation should handle, store and delete police data according to the Government Security Classifications. The table below provides further guidance on the GSC.

Organisations that already have security procedures in place that afford data the same protection as the GSC controls should apply the same regulations to data disclosed by Lincolnshire Police or any other partner organisation.

### Transmitting information securely

When sharing information both the sender and the receiver should deal with the information according to its protective marking. See Government Security Classifications table below for handling requirements in line with information classification.

Any e-mail or attachment containing personal data must be sent via a secure encrypted e-mail system. Where the partner does not have access to a secure encrypted e-mail system, the information must be encrypted via some other means, such as Windows password encryption, and the password sent via other means, such as telephone.

## Government Security Classification – Control Measures at OFFICIAL

|  |  |
| --- | --- |
|  | OFFICIAL including OFFICIAL-SENSITIVE |
| Personnel Security  | * All staff, volunteers, contractors etc. must have appropriate vetting clearance
 |
| Physical Security a. Document handling  | * No requirement to mark documents with **OFFICIAL** marking
* Comply with the Clear Desk – Clear Screen policy
* **OFFICIAL-SENSITIVE** the document must be marked at the top and bottom of each page and handling instructions considered, e.g.
	+ FOR POLICE EYES ONLY
	+ TO BE OPENED BY ADDRESSEE ONLY
	+ NOT FOR FORWARD DISSEMINATION
	+ NO PHOTOCOPYING WITHOUT PERMISSION OF ***AUTHOR***
 |
| b. Storage  | * Storage behind a single locked barrier. **OFFICIAL – SENSITIVE** – consider a second locked barrier.
* **OFFICIAL-SENSITIVE** - Consider use of approved physical security equipment/furniture (Contact Information Security Officer in PSD for advice)
 |
| c. Remote Working  | * Ensure information cannot be inadvertently overlooked whilst being accessed remotely
* Store assets under lock and key at remote locations
 |
| d. Moving assets by hand | * Single cover with no external markings – sealed transit envelope is acceptable
* **OFFICIAL-SENSITIVE** – Sealed envelope – no external markings
* Precautions against overlooking when working in transit (e.g. whilst travelling by train)
 |
| e. Moving assets by post/courier  | * Sealed envelope, never mark classification on envelope
* **OFFICIAL-SENSITIVE** - Consider double enveloping
* If sending sensitive personal data externally use registered Royal Mail service or reputable commercial courier’s ‘track and trace’ service
 |
| f. Moving assets overseas  | * Sealed envelope, include return address, never mark classification on envelope
* Trusted hand under single cover (Contact Information Security Officer in PSD for advice)
 |
| g. Bulk Transfers  | * Authorisation from Information Asset Owner required for significant volume of records/files
* Contact Force Information Security Officer for advice and risk assessment
 |
| INFORMATION SECURITYa. Electronic Information at Rest  | * Electronic data at rest can be found on computers, mobile devices etc. This information is protected according to its sensitivity; for portable devices data will be encrypted.
* Appropriate controls to protect the information may be physical protection, such as a locked door or may involve encrypting data that would be classified as **OFFICIAL-SENSITIVE**
 |
| b. Electronic Information in Transit e.g. e-mail | * Remember, ALL emails are at least **OFFICIAL**
* Information between Police forces, government and trusted organisations is via secure networks.
* If the email does not contain sensitive information, you can send it over the insecure internet e.g. anyone@anywhere.com
* Do not send sensitive information to insecure internet domain addresses, such as Google mail, Hotmail, Yahoo, consider redacting the information if appropriate
* Where more sensitive information must be shared with external partners or members of the public, consider using secure mechanisms such as password protected documents. Consider file encryption for **OFFICIAL-SENSITIVE** together with handling instructions.
* Where more sensitive information must be shared with external partners, ensure secure mechanisms (e.g. browser sessions using SSL/TLS) are used. Consult the Information Security Officer in PSD for advice
* You should provide handling instructions, if necessary, based on your risk assessment and at **OFFICIAL-SENSITIVE**
* In **exceptional** circumstances, where there is a requirement for information to be sent unencrypted over the Internet, you have to make a risk-balanced decision; there is always a risk of information being intercepted and exposed. It is very important to stipulate handling instructions in this scenario.
* You must follow any handling guidance stipulated by the relevant Force Information Asset Owner
 |
| c. Removable Media (data bearing) | * All portable and removable media must be encrypted and only Force supplied devices are to be used
* Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement
 |
| d. Telephony (mobile and landline), Radio, Video Conference and Fax  | * Details of sensitive material should be kept to a minimum – be aware of being overheard and your surroundings
* Your conversation, video conference etc. may be recorded by the other or a third party
* Faxing is only acceptable as a last resort, where the recipient does not have a secure e-mail and there isn’t time to send via post
* Recipients should be waiting to receive faxes containing personal data and/or data marked with the **OFFICIAL – SENSITIVE** caveat
 |
| Disclosure | * Where appropriate, non-sensitive information should be published by the Force for reuse.
* Statutory disclosures are separate from the classification scheme and require case-by-case assessment
* Requests for release under the Freedom of Information Act should be referred to the Freedom of Information Unit
* The release of personal data is subject to the Data Protection Act principles. Contact the Data Protection Unit for advice.
 |
| Destruction of Hard Drives etc. | * All disposal of IT equipment must be carried out by the Information Services Department
 |
| Disposal / Destruction of paper  | * Destroy using equipment which meets a recognised international paper destruction standard, designed to consistently destroy to particles no larger than 4 x 15 mm
 |
| Incident Reporting  | * Inform your line manager and complete the relevant Force Incident reporting form
* Follow incident reporting procedures set out in the relevant Force Security Policy
 |

## Appendix 4 - Lincolnshire Children’s Services Request For Police Disclosure Form

**** 

**REQUEST FOR POLICE DISCLOSURE**

|  |
| --- |
| **REASON FOR REQUESTING DISCLOSURE FROM POLICE** |
| **URGENT****Emergency placement of child or safety plan requiring adult to immediately supervise or support care of child.** | **If yes, please send completed form to: -** **LPSH@lincs.police.uk****Please select as necessary if neither of these go to non-urgent process.**[ ]  **Emergency Placement (for immediate placement)**[ ]  **Safety plan for immediate supervision requirements** |
| **NON-URGENT – Maximum 10 working days****Planned placements/police check as part of viability assessment.****Agency check within child and family assessment or plan (CS – see criteria)** | **Please send any non-urgent to: -****disclosurehq@lincs.police.uk****Please select as necessary**[ ]  **Police disclosure**[ ]  **Specific additional request following police disclosure – provide details.** |

|  |
| --- |
| **REQUESTER DETAILS** |
| **NAME AND ROLE** |  |
| **EMAIL ADDRESS OF SOCIAL WORKER** |  |
| **EMAIL ADDRESS OF TEAM ASSISTANT** |  |
| **DATE** |  |

|  |
| --- |
| **CHILD DETAIL THAT DISCLOSURE RELATES TO** |
| **CHILDREN** |
| **Names** |  |

|  |
| --- |
| **SUBJECT DETAILS**  |
|  | **PERSON 1** | **PERSON 2** | **PERSON 3** |
| **Forename** |  |  |  |
| **Surname** |  |  |  |
| **Previous Names or Alias** |  |  |  |
| **Date of Birth** |  |  |  |
| **Place of Birth** |  |  |  |
| **Current Address** |  |  |  |
| **Other Addresses (last 5 years)** |  |  |  |

***If your request is for more than 3 people, please copy, and paste table above to add additional persons. You do not need to complete a different from.***

## Appendix 5 - Lincolnshire Children’s Services and Lincolnshire Police Protocol on Managing Domestic Abuse Notifications & Referrals where Children are involved/resident in the Household

1. **Purpose**

To lay out the procedure for informing Lincolnshire Children’s Services of any domestic abuse incidents that come to the attention of Lincolnshire Police that concern children.

The aim is to increase the effectiveness of passing information concerning incidents of domestic abuse distinguishing

1. Referrals that need an immediate response by Children’s Services
2. Notification of incidents which will be taken as information only by Children’s Services until there are 3 such notifications in a rolling year or there are other referrals
3. Requests for further information from Children’s Services i.e. copies of Domestic Abuse Stalking & Harassment (DASH) forms.
4. **Safeguarding Responsibilities**

Safeguarding of children and/or vulnerable adults should be at the forefront of the mind of all officers and staff. When responding to domestic violence or abuse incidents, Lincolnshire Police Officers must complete the DASH form to the fullest. This assesses the risk to the adult victim (aged 16 or over) in the situation but does not specifically determine the risk to children.

The Police Force Control Room (FCR) must ensure that all incidents of domestic abuse are correctly closed using appropriate codes.

**In general, factors which should raise concerns about the safety and welfare of children when Police attend domestic abuse incidents include:**

* An alleged victim is a child.
* The children have witnessed or have been distressed through hearing incidents of domestic abuse
* When a child is used as a shield
* When a child is injured
* When a child has called the police
* When a case is referred to MARAC and children are a member of the household
* Where the officer’s professional judgement is that there are other risks of significant harm to a child

In any case where emergency protection is required, the attending officer will take appropriate action.

The police officer should advise parent/carer verbally as early as possible that the information from the DASH will be shared with other agencies – there is a reminder of this on the DASH form.

**IN ALL CASES REMEMBER: Live CPR checks are available, for all officers, regardless of the DASH risk outcome, if they have a concern for the child and require further information to inform their decision-making process. They are not compulsory, but if completed should be done so at the scene by the attending officer.**

1. **Outline of Processes Agreed between the Agencies**
	1. **General Guidance for Police Officers to refer Children where there is Domestic Abuse**

Attending officers must ensure they include all details of children involved within the family in the Public Protection Notice form, regardless of if they were present during the incident or not. The Attending Officer can make a referral to Lincolnshire Children’s Services on any case regardless of risk if they have specific concerns about the safety or welfare of a child. This should be done via the Public Protection Notice form available via the Mobile Data Terminal, Pronto and Niche.

Officers are made aware that there is one point of referral in Lincolnshire and that is Customer Service Centre (CSC). All DASH risk assessments that are categorised as high risk are automatically shared with the Customer Service Centre via Niche. The notification provides a copy of the DASH and the details of all involved and the circumstances of it providing it is included within the PPN. The LPSH, through the Support and Research staff, will manage all Standard and Medium DASH referrals, through the Public Protection Notice process. These will be reviewed, and where appropriate updated with any additional children or other persons that are identified as being relevant to any safeguarding concerns. They will then be shared, electronically with Lincolnshire Children’s Services. Onus will always be in the attending officer to ensure all relevant child details are obtained.

Should any officer take immediate safeguarding action for a child, at a domestic abuse incident, where they consider them to be at risk of immediate significant harm, they should follow the Police Protection procedure, with Inspector authorisation.

During working hours they should contact LPSH for support 01522 212365 and out of working hours Emergency Duty Team (EDT) on 01522 782333.

**3.2. Police Referrals from LPSH to Lincolnshire Children’s Services Customer Service Centre (CSC)**

LPSH will use the electronically generated referral form to process all referrals with Lincolnshire Children’s Services CSC.

A copy of the latest DASH is automatically included in all referrals from LPSH to CSC on domestic abuse incidents regardless of the risk grading.

Most of these DASH forms will be completed by frontline response officers. They will be completed with the identified victim at a safe location.

**3.3 Domestic Abuse Referrals from Lincolnshire Police to Children’s Services**

In incidents where Lincolnshire Police have identified a concern for the safety or wellbeing of a child information will be shared with Lincolnshire Children’s Services electronically on secure email to CSC\_Childrens\_Team@lincolnshire.gov.uk.

**Responses from Lincolnshire Children’s Services to referrals.**

1.Referrals will be processed by staff at Customer Service Centre (CSC). All referrals will be added as a contact and sent to the Screening Team for review.

2. If the referral refers to a child/ren who are open to any Children’s Services team this will be passed to the key worker and team manager by the Customer Service Centre

3. All referrals will be screened within 1 working day by the Children’s Services Screening Team and actions determined within that timescale.

4.Children’s Services will notify Lincolnshire Police of the outcome of all referrals. These are managed by the Support and Research staff within Lincolnshire Police and added to the corresponding Niche under occurrence report titled ‘Confidential Outcome’

5. The Team Manager or Practice Supervisor may contact the LPSH for clarification of information and/or a strategy discussion

**3.4.** **Domestic Abuse Notifications from Lincolnshire Police to Children’s Services**

**Standard and Medium Risk DA Incidents where Lincolnshire Police have no specific concerns for the safety or welfare of a child/ren.**

In incidents of standard and medium risk where Lincolnshire Police have no specific concerns for the safety or welfare of a child other than the existing Domestic Abuse situation, information will be shared with Lincolnshire Children’s Services via LPSH direct to Lincolnshire’s Children’s Services electronically on secure email to CPRUAdmin@lincolnshire.gov.uk within 72 hours of the incident (noting bank holiday weekends and LPSH cover)

**Responses from Children’s Services to Notifications of Standard and Medium Risk DA Incidents where Lincolnshire Police have no specific concerns for the safety or welfare of a child/ren.**

1. All notifications will be processed by administrative staff at Children’s Services Safeguarding Unit. The notification will be added as a domestic abuse contact. There will be no further action undertaken by Children’s Services unless there have been three or more notifications in a rolling 12-month period.
2. If there has been three or more standard or medium domestic abuse notifications in a rolling 12-month period, the Safeguarding Unit will send the last contact through to the CS Front Door Screening Team who will determine if there is an identified safeguarding concern and a need for a Social Care Assessment to be undertaken.
3. Where a notification refers to a child/ren who are open to any Children’s Service’s team, this information will be shared with the responsible key worker and Team Manager by the Safeguarding Unit.
4. Children’s Services will not notify Lincolnshire Police of the outcome of notifications unless progressed for a Social Care Assessment and further intervention is required from the Police.
5. Notifications sent to the Screening Team due to meeting the trigger set out at 1. Above will be screened within 1 working day and actions determined within that timescale.
6. The Team Manager or Practice Supervisor may contact the LPSH for clarification of information and/or a strategy discussion

**3.5 Requests for information from Lincolnshire Police when a social worker is undertaking a Child and Family Assessment (CFA)**

Current practice is that when a social worker is completing a CFA, they should gather information from all agencies including police.   Police information is gathered, after consent is obtained from the Police Information Management Unit (IMU) utilising the agreed Information Sharing Agreement (ISA) and request form.

1. **Other information**
* The DASH is shared with Lincolnshire Children’s Services via Niche, in an electronic format and is shared using a secure email.
* The initial DASH provided by LPSH, from DA incidents, will be that completed, generally, by the initial response officer. In cases where immediate safeguarding is required, the Officer or OIC will be working closely with Children’s Services and information will be shared and documented accordingly.
* Historic DASH forms will not be provided by Lincolnshire Police. DASH is a dynamic risk identification, assessment, and management process. Lincolnshire Children’s Services will complete DASH forms to assess and continually assess current risks of serious harm to enable management of cases effectively.
* The Information Sharing Agreement (ISA) reflects that Lincolnshire Children’s Services will ensure that the police provided DASH is saved confidentially and is not shared with any other agencies, third party, or for example the alleged perpetrator. The purpose of sharing the DASH, in the circumstances outlined in this protocol, is to inform the Social Care Assessment (SCA) and any subsequent safety plan put in place.

**5. Senior Management Undertaking.**

These new processes started within August 2016. The two agencies senior management will ensure.

* That all required parties to the Protocol have been briefed accordingly
* All required parties understand the processes they should use to share and request information securely in line with the update Information Sharing Agreement (ISA)
* The protocol will be reviewed between the two agencies every 6 months going forward.

**6. Signatories to this Protocol:**

|  |  |
| --- | --- |
| Signed on behalf of Lincolnshire Police: | Signed on behalf of Lincolnshire Children’s & Family Services: |
| Kam Mistry |  |
| Role: D/Superintendent, Head of PVP | Role: Assistant Director, Children’s Services  |
| Date: 20th January 2025 | Date: 24th February 2025 |