Lincolnshire Police

Information Sharing Agreement

Information Sharing Agreement (ISA) between

Lincolnshire Co-Operative Limited

and

Lincolnshire Police

Version: 6.0

(Revised – 26th Nov 2024)

Summary Sheet

Reference number: LP005/LWL – Lincolnshire Co-operative Limited

Purpose

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

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

This agreement will determine the named parties' responsibilities in relation to relevant legislation including, but not limited to, Data Protection Legislation. It assists to enable parties 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 Co-operative Ltd, Lincolnshire Co-operative Ltd, Stanley Bett House, 15/23 Tentercroft Street, Lincoln, Lincolnshire, LN5 7DB

Date Agreement comes into force:	1st November 2013
Date of Agreement Review:	Six months after coming into force, then annually
Agreement Owner:	Lincolnshire Police
Agreement drawn up by:	E.D Tedder – IS Officer – Lincolnshire Police
Location of Signed Agreement:	Information Management Unit, Force HQ

Version History

Version No.	Date	Amendments Made	Authorisation
001	12 Feb 13	Initial Draft	E D Tedder - IS Officer
002	22 Aug 13	Amendments made to draft	L Chapman – IS Officer
1.0	24 Oct 13	Authorised	L Chapman – IS Officer
2.0	24 Jun 14	Appendix 3 Amended to reflect legislative changes to Rehabilitation Periods.	L Chapman – IS Officer
3.0	23 Mar 18 03 Apr 18	Para 9.9 amended due to adoption of the Government Security Classification. Appendix 2 amended due to adoption of the Government Security Classification. Para. 8.1 amended: SPoC details updated.	L Chapman – IS Officer L Chapman – IS Officer
4.0	29 May 20	Revised template adopted due to the enactment of revised Data Protection Legislation.	L Chapman – IS Officer
5.0	21 Apr 22	Agreement reviewed, latest template adopted, minor amendments made.	L Chapman – IS Officer
6.0	20 Mar 24 21 Nov 24	Agreement reviewed; latest template adopted. SPoC contact details updated. Information	D Stenner – IS Officer D 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 action to be taken against crime and anti-social behaviour. It will incorporate measures aimed at:

- Facilitating a coordinated approach that targets crime and anti-social behaviour;
- Facilitating the collection and exchange of relevant information;
- Ensuring that the sharing of information meets one or more of the policing purposes in conjunction with the Law Enforcement purposes.
- Where appropriate, the pursuit of criminal or civil proceedings – either by The Chief Constable or Partners to this agreement

2. Specific Purpose

2.1 Aims and Objectives

The aim of the Co-operative Shopwatch initiative is to reduce retail theft and antisocial behaviour by sharing information regarding relevant prolific offenders. This will ensure that shopping areas are safer for customers and staff.

2.2 Context of the processing

Relevant information will be shared when it is identified that a prolific offender has been banned from the premises managed by Lincolnshire Co-operative in order for staff to identify such offenders. The sharing of photographs and relevant incident information will fulfil the purpose of the agreement by ensuring that staffs are aware of the prolific offenders that have been banned from Lincolnshire Co-operative premises, therefore aiding in the prevention of retail theft.

3. Types of Information to be Shared

3.1 Lincolnshire police may share:

- Evidence relating to a conviction for an offence or alleged offence associated with Theft, Burglary, Robbery and Fraud, providing that the conviction is not considered spent under the Rehabilitation of Offenders Act 1974, see Appendix 2;
- Evidence relating to a conditional caution accepted by an accused for an offence associated with Theft, Burglary, Robbery and Fraud offences, where the date of the caution is less than three months from the disclosure date; providing that the conditional caution is relevant to the request and the disclosure of information can be justified on the grounds that it falls within a policing purpose.

- Information between the two parties will be exchanged for the sole purpose of preventing and detecting crime relating to Theft, Burglary, Robbery and Fraud offences.
- Photographs of individuals convicted of Theft, Burglary, Robbery and Fraud offences, where current information/intelligence suggests that they may still be active within the Lincolnshire Police area, providing that the information is relevant to the request and the disclosure of information can be justified on the grounds that it falls within a policing purpose.

3.2 Lincolnshire Co-operative may share

- Information / evidence received involving the offences of Theft, Burglary, Robbery and Fraud occurring in or affecting the Lincolnshire Police area.
- Evidence from internal shop CCTV schemes (where they exists) in relation to offences committed therein.

3.3 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".**

3.4 Information must only be shared on a 'need to know' basis.

3.5 Prior to disclosure, consideration to the Rehabilitation of Offenders Act 1974 regarding spent convictions may be required; this will be dependent on the purpose of the agreement. See Appendix 2 for further information regarding spent convictions.

4. The Sharing Process

4.1 Relevant photographs will be supplied by Lincolnshire Police to Lincolnshire Co-operative Ltd on a regular basis, providing that they are supported with a Form B (P698B) – Response to Request for Information,

which must be retained by the Police SPoC within the file created for such purpose.

4.2 If additional information is required Lincolnshire Co-operative Ltd must make their request in writing using Form A - Request for Personal Information.

4.3 Requests and responses to requests should be done via a secure/ encrypted messaging system. The decision to provide information will be documented on Form B - Response to Request for information. Copies of both Form A and Form B will be retained by the Police SPoC within the file created for such purpose.

4.4 Replies to requests must be made within ten working days.

4.5 Any photographs provided will not be displayed in any public areas of the premises but will be retained within the 'private' parts of the premises so that they can only be viewed by the licensee and bar staff/door supervisors. The photographs should be locked behind a least one barrier.

4.6 Once the reason for the supply of the photograph is no longer valid, the photograph will be destroyed by the licensee or returned to the Police SPoC.

4.7 If the disclosures are completed by email this 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.

4.8 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.

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:

Lincolnshire Police SPoC
Title: Neighbourhood Inspector Lincoln North East
Contact Details: daniel.gilmore@lincs.police.uk Mobile: 07867906085

Lincolnshire Co-operative Ltd SPoC
Title: Co-operative Security Manager
Contact Details: 01522 504514

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.

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

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 Poling 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:

a. Prevention, investigation, detection or prosecution of criminal offences
b. Execution of criminal penalties
c. 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 3 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 is for Law Enforcement Processing and non-Law Enforcement Processing, therefore the following lawful basis(es) applies for the processing of personal information.

Law Enforcement Processing between Competent Authorities

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:

- The exercise of a function conferred by an enactment or rule of law and is necessary for reasons of substantial public interest.
- The administration of justice.

All partners to this agreement 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):
- Article 6 (1) (f) Legitimate interests: the processing is necessary for the purposes of the legitimate interests pursued by the data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which required protection of personal data, in particular where the data subject is a child.

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:
- 9(2)(g) - Substantial public interest/rule of law (DPA 2018 Schedule 1, Part 2) 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 condition selected 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 and detecting unlawful acts
11) Protecting the public

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), from Schedule 1 Part 2:

10) Preventing and detecting unlawful acts
11) Protecting the public

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) by virtue of the DPA (2018) Part 2: (10) (11)

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

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:

- Prevention of disorder or crime

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 Lincolnshire Police and the Lincolnshire Co-op have Privacy Notice's in place which are available on the internet. 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 Co-op is to effectively deal with issues concerning the prevention, detection, investigation and prosecution of those persons engaged in criminal activity and/or anti-social behaviour, and an ongoing responsibility to protect public safety.

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 4 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.

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
- Protecting the public against dishonesty
- Preventing fraud

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 erasure of data.
- 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 Co-Operative Limited - dataprotection@lincolnshire.coop or kemi.Adewole@lincolnshire.coop

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: *Original signed*

Name:

Rank/Position: Assistant Chief Constable

Date: 26th November 2024

Signed on behalf of Lincolnshire Co-op

Sign here: *Original signed*

Name:

Rank/Position: Security Manager

Date: 25th November 2024

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)) –

   a. the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
   b. the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
   c. the processing of data concerning health;
   d. 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 - Rehabilitation Periods

1. Prison sentences of more than four years never become spent.

2. The rehabilitation periods for the main sentences are set out in the table below:

Sentence	End of rehabilitation period for adult offenders	End of rehabilitation period for offenders under 18 at date of conviction
A custodial sentence of more than 30 months and up to, or consisting of, 48 months	The end of the period of 7 years beginning with the day on which the sentence (including any licence period) is completed	The end of the period of 42 months beginning with the day on which the sentence (including any licence period) is completed
A custodial sentence of more than 6 months and up to, or consisting of, 30 months	The end of the period of 48 months beginning with the day on which the sentence (including any licence period) is completed	The end of the period of 24 months beginning with the day on which the sentence (including any licence period) is completed
A custodial sentence of 6 months or less	The end of the period of 24 months beginning with the day on which the sentence (including any licence period) is completed	The end of the period of 18 months beginning with the day on which the sentence (including any licence period) is completed
Removal from His Majesty's service	The end of the period of 12 months beginning with the date of the conviction in respect of which the sentence is imposed	The end of the period of 6 months beginning with the date of the conviction in respect of which the sentence is imposed
A sentence of service detention	The end of the period of 12 months beginning with the day on which the sentence is completed	The end of the period of 6 months beginning with the day on which the sentence is completed
A fine	The end of the period of 12 months beginning with the date of the conviction in	The end of the period of 6 months beginning with the date of the conviction in

	respect of which the sentence is imposed	respect of which the sentence is imposed
A compensation order	The date on which the payment is made in full	The date on which the payment is made in full
A community or youth rehabilitation order	The end of the period of 12 months beginning with the day provided for by or under the order as the last day on which the order is to have effect	The end of the period of 6 months beginning with the day provided for by or under the order as the last day on which the order is to have effect
A relevant order	The day provided for by or under the order as the last day on which the order is to have effect	The day provided for by or under the order as the last day on which the order is to have effect

3. Where no provision is made by or under a community or youth rehabilitation order or a relevant order for the last day on which the order is to have effect, the rehabilitation period for the order is to be the period of 24 months beginning with the date of conviction.

4. There is no rehabilitation period for:

    a. An order discharging a person absolutely for an offence, or
    b. Any other sentence in respect of a conviction where the sentence is not dealt with in the Table above or where no provision is made by or under a community or youth rehabilitation order or a relevant order.

    In such cases mentioned above, any rehabilitation period is to be read as if the period of time is nil.

    For example, a caution becomes spent immediately, and a conditional caution becomes spent after three months from the date on which the caution is given, or, if earlier, when the caution ceases to have effect.

5. Consecutive terms of imprisonment or other custodial sentences are to be treated as a single term,

6. Terms of imprisonment or other custodial sentences which are wholly or partly concurrent (that is terms of imprisonment or other custodial sentences imposed in respect of offences of which a person was convicted in the same proceedings) are to be treated as a single term.

For further information on the rehabilitation periods, see Chapter 8 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012, which can be accessed using the following link:

http://www.legislation.gov.uk/ukpga/2012/10/part/3/chapter/8/enacted

Appendix 3 – 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 4 - 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:

a. No unencrypted laptops or drives or removable electronic media containing personal information should be taken outside office premises.
b. 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:

a. Does the data controller have a security policy setting out management commitment to information security within the organisation?
b. Is the responsibility for the organisations security policy clearly placed on a particular person or department?
c. 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 SECURITY **a. 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