Safer Lancashire Community Safety Information Sharing Protocol

June 2022

Guidance for creating Information Sharing Agreements for organisations involved with Community Safety across Lancashire

Commissioned by the Lancashire Community Safety Partnership Board

Document Control

Version:	1.3
Date:	June 2022
Author:	Debbie Thompson, Public Health Specialist (Stronger and Safer Communities) Health Equity, Welfare and Partnerships
Document Owner:	Lancashire Community Safety Partnership Board
Approving Committee:	Lancashire Community Safety Partnership Board
Review Date:	March 2023
Document Classification:	**PUBLIC**

Change History

Version:	Date:	Contributor / Author:	Description of Change:
1.0	February 2021	Russell Walton	Document Creation
1.1	March 2021	Adam Hillhouse	Removal of LCC branding and retitling of document. GDPR updated to UK GDPR.
1.2	June 2021	Alison Wilkins	Incorporated changes from Head of Data Protection & DPO, Lancashire Constabulary
1.3	June 2022	Alison Wilkins	Incorporated changes from Head of Data, Digital Services, Lancashire County Council

Acknowledgements

We would like to thank the Derbyshire Partnership Forum and the Safer Warwickshire Partnership Board for their assistance in the production of this document.

Contents

1. Introduction

The Lancashire Community Safety Partnership Board aims to create safer communities through the reduction of crime and the promotion of safety.

The Board is responsible for putting in place a protocol to facilitate information sharing between responsible authorities for community safety in Lancashire. All responsible authorities, statutory agencies, the Office of the Police and Crime Commissioner and other groups providing community safety in the county ("partner agencies") agree to the protocol.

Responsible authorities as detailed by the Crime and Disorder Act 1998 are:

- County council, district council, borough council or unitary authority.
- Police.
- Fire and Rescue Authorities.
- Health – Integrated Care Board
- Probation Services.

The purpose of this information sharing protocol is to set out a framework for partner organisations and their staff to process, share personal and sensitive personal information on a lawful, fair and transparent basis with the purpose of enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.

All organisations play a role in supporting the sharing of information between and within organisations and address any barriers to information sharing to ensure that a culture of appropriate information sharing is developed and supported.

This document sets out the principles and commitments that will underpin the secure and confidential sharing of information between organisations involved in delivering services to people living and working within Lancashire. The document contains a template to create **Information Sharing Agreements (ISAs)** (see **Appendix 14**) between partner organisations where multiagency meetings and data sharing occurs.

The protocol reflects the new General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018.

2. Purpose of the Information Sharing Protocol

The purpose of this protocol is to facilitate the lawful exchange of information, other than anonymised information. To comply with the statutory duty placed on the responsible authorities to work together to develop and implement a strategy and tactics for reducing crime and disorder, anti-social behaviour and substance misuse. This includes when an individual poses a risk of harm to the community, other individuals at risk or professionals and any other behaviour affecting the local environment.

Specifically, this Protocol aims to:

- Set out generally what information is shared personal data.
- Set out the general principles of information sharing.
- Identify the lawful basis for sharing information.
- Define the common purposes for holding and sharing data.
- Promotes a standard approach to the development of Information Sharing Agreements.
- Set out how information will be stored.
- Identify the partner organisations who are signatories to this Protocol.

This Protocol applies to chief officers, elected members, executive directors, non-executive directors, trustees and all employees including volunteers and agency staff of the organisation and partner organisations who are signatories.

The Protocol also applies to any organisation or agency, commissioned to deliver services on behalf of any organisation party to this Protocol subject to granted permission to the third party organisation to disclose information by consent of the Controller.

The Protocol is intended to complement any existing professional Codes of Practice that apply to any relevant profession working within any organisation including the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA), but does not cover an individual organisations compliance to the UK GDPR or DPA and does not constitute legal advice. See **Appendix 8** for a list of non-exhaustive relevant legislation that may affect your ability to share information.

Partners should consider the likely effect of not sharing information, for example, harm to individuals, damage to their organisations' reputation, disconnect in partnership working and lack of understanding of problems.

3. Information Sharing Principles

In the interests of fairness and transparency, partners agree to the following principles:

- The sharing of personal information is in a lawful manner.
- Any Shared Personal Data, including special category data and criminal offence data is in accordance with the data protection principles, UK GDPR and Data Protection Act 2018.

The principles established by this Protocol make sure personal information is:

- Used fairly, lawfully and transparently.* (*Transparency is not always necessary in relation to processing for law enforcement purposes).
- Used for specified, explicit purposes.
- Used in a way that is adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

4. Commitments in Support of the Protocol

Signatories to this Protocol are committed to the implementation of an appropriate level of Information Governance throughout their organisation, in accordance with recognised national standards. To achieve these principles, Partner organisations agree to:

- Adhere to the principles and commitments of this Protocol whenever exchanging personal information, whether with a co-signatory or other agency/organisation.
- Share statistical and anonymised/pseudonymised data wherever possible, eliminating the use of personal information except where reasonably necessary.
- Ensure that all staff (including temporary employees, contractors and volunteers) are aware of and comply with their responsibilities arising from both the Protocol and relevant legislation, and receive adequate training in order to do so.
- Implement their own policies on confidentiality, data protection, information security, records management and information quality, which are appropriate to their organisation and comply with recognised codes of practice.

Signatories to this Protocol will also establish efficient and effective procedures for:

- Obtaining, informed consent to collect, share and process personal information wherever reasonably practicable and where appropriate.
- Informing individuals what information is collected and shared about them.
- Sharing of personal information identified as part of a detailed agreement.
- Addressing complaints arising from the misuse or inappropriate disclosure of personal information arising from information sharing decisions.
- Enabling access to records of individuals by those individuals on request.
- Amending inaccurate records and informing partners where these are shared.
- Review and destroy information in accordance with good records management practice and organisational policy.
- Sharing information without consent when necessary, recording the reasons for that disclosure (including legal basis) and the person responsible for making the decision.
- Making information sharing an obligation on staff and allocating senior staff responsibility for making complex disclosure decisions.
- Protecting personal information at all times, with appropriate protective marking, security and handling measures and in accordance with the Government Security Classifications.
- Develop and work to detailed, specific information sharing agreements that support identified purposes.
- Ensure that future developments in technology reflect the requirements of the UK GDPR, DPA 2018 and this Protocol and any that any information sharing is secure and can comply with the UK GDPR and DPA.
- Issues, incidents and complaints resulting from failures in the specific agreements feed into the review processes for the individual agreements.
- Share information free of charge unless special charging arrangements are agreed.
- Seek legal advice where appropriate.

- Ensure their registration as Controllers under the DPA 2018 is adequate for the purposes for which they may need to process and share information with one another.
- Support the principles of equality and diversity within the community. Ensure that information provided to the public is in appropriate formats and languages.
- Support the technical transportation in sharing data, working actively with partners to identify the most appropriate solution available to partners to consume data in the most continuous repeatable method.
- Ensure that all assured datasets are published to a data catalogue to allow partners to understand the data available and understand how the data can be applied.

The organisations signed up to this Protocol are fully committed to adhering to these principles at all times.

5. Who will be Sharing Information?

Partners who are required to share information are the responsible authorities in the 1998 Crime and Disorder Act, as amended in the 2006 Police and Justice Act and 2009 Policing and Crime Act. These are the Police, all Local Authorities, Fire and Rescue Service, Integrated Care Partnerships and National Probation Service.

Co-operating bodies under the Act may be asked to share information. These are the Parish Councils, School and College Governing bodies, Registered Social Landlords and agencies appropriate to the location or circumstances.

Various other bodies as invited participants under the Act and who may be asked to share data for crime and disorder purposes.

Wider partners may also be required to share information in specific circumstances. These could include schools, other health agencies and voluntary sector organisations.

Collectively, these organisations are referred to as “Partner agencies”. The Lancashire Community Safety Partnership Board approves this protocol. Member organisations of this Board sign up to the principles of the protocol by virtue of their membership. Other partners can formally sign up to the protocol. To do so, or to check if an agency has signed up to the protocol, please email **communitysafety@lancashire.gov.uk**

Where an agency has not signed up to the protocol, but a partner/partners wish to share Shared Personal Data with them, extra care is required to ensure they understand the sharing and handling of sensitive information they see. It may be necessary to provide a specific instructions and handling arrangements and ensure the agency representatives sign a confidentiality agreement to confirm that they understand their responsibilities. See **Appendix 13** for a sample confidentiality agreement.

6. The Sharing of Information

The 'Delivering Safer Communities' guidance and the Crime and Disorder Act 2008 place a duty upon relevant authorities to share information. Additionally, Partner agencies have express and/or implied powers to share information as set out in legislation. (See **Appendix 8** for a non-exhaustive list of legislation.)

Shared Personal Data will usually include information about the nature of the problem and, where relevant, personal data such as names addresses and dates of birth of offenders, victims or witnesses.

Most of the Shared Personal Data will also include sensitive/special category/criminal offence personal data as defined in data protection legislation. Sharing of this type of sensitive information is allowed in lawful and appropriate circumstances. Any sharing of personal data including sensitive data known as special category data or criminal offence data must be undertaken in accordance with UK GDPR and Data Protection Act 2018.

In order to share appropriate information between partners there must be a lawful, defined and justifiable purpose(s), which supports the effective delivery of a policy, or service that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This agreement, supplemented by a number of questions, included at **Appendix 12**, is designed to support Managers/Designated Persons and other specialist support through a process to assess the impact and appropriateness of information sharing.

'Signatories' to this protocol understand that Shared Personal Data will be shared at multi-agency meetings (see **Section 6**). For example, there may be meetings between members of staff from different agencies sharing information about a common case in order to build a foundation of accurate knowledge and evidence, to minimise the risk of harm to the community, whilst allowing proper management of the case. The intention of this protocol is to cover all such information sharing.

If any Shared Personal Data relates to an ongoing investigation or prosecution by any of the agencies then consultation must take place with the investigating officer and Crown Prosecution Service as the matter will be sub-judice. This will ensure that disclosure will not adversely prejudice the outcome of the matter.

Take special care when considering the sharing of information that could constitute profiling, particularly of children. A legal justification must be available before sharing any sensitive information.

7. Arrangements for Data Sharing within Multi-Agency Meetings

Using the definitions in **7.1** of this agreement the chair of each meeting should designate the level of confidentiality appropriate to the information shared at the outset. Where relevant, they must provide a confidentiality declaration sign-in sheet (**Appendix 13**) which states the data sharing requirements relevant to the meeting

and highlight the restrictions or limitations in relation to the use of the information. If used, the chair should securely retain a copy of this confidentiality declaration sign-in sheet.

The parties to this protocol understand that in keeping with government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the Crime and Disorder Act 1998, it is likely that there will be individuals present at certain meetings who are not representing an organisation that is a signatory to this protocol. To allow for this, the signing-in sheet should state that the signatory agrees to abide by all the terms of this protocol.

It is good practice to use the Government Security Classifications. These set out levels of confidentiality and appropriate security measures that should be applied to information assets. These classifications are the method by which the originator of an asset (all material assets, i.e. papers, drawings, images, disks and all forms of electronic data records) indicates to others the levels of protection required when handling the asset in question. This includes terms of sensitivity, security, storage, movement both within the guidance and outside the originator's own department or force and its ultimate method of disposal.

7.1 The levels of classification are:
Official: All routine public sector business, operations and services.

Official – Sensitive: A limited subset of **Official** information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. In cases where there is a clear and justifiable requirement to share only on a need to know basis, the **Official – Sensitive** classification should be used.

Secret: Very sensitive information where compromise would directly threaten an individual's life, liberty or safety or cause serious damage to the effectiveness or security of the UK.

Top Secret: Exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies.

The chair of each multiagency meeting is responsible for ensuring the confidentiality declaration sign-in sheet is kept current and as far as they are able to, includes all legal requirements surrounding information sharing.

8. Process for Data Sharing Outside Meetings

This Protocol is to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case.

Information must be requested in a legally compliant manner, setting out the legal grounds for disclosure, for example if the Crime and Taxation exemption under the Data Protection Act (DPA) 2018 Schedule 2 Part 1 (2) is being relied on, then this should be formally set out and the specific details required. Where relevant, use

access request forms, or alternative official third party subject access request forms (where required by other partners).

Privacy Notices and Record of Processing Activity (ROPA) reports should make clear where sharing of information shared will occur. Information shared should only be used for the purpose requested by the requesting partner and should not be shared further without consent of the information owner unless there is a legal obligation or other lawful basis for doing so.

Any sharing and storing of data must be in accordance with the relevant legislation. In particular, when sharing personal data, use a secure transmission system, such as secure email or courier or hosted on a secure system shared by partners. All Partner agencies must have appropriate technical and organisational measures in place, having regard to the nature and sensitivity of the information, to ensure information security. This will include monitoring and auditing procedures as well as the ability to respond to any failure to adhere to the data sharing Protocol swiftly and effectively and to report any personal data breach.

Only keep information as long as it is necessary. All signatories must confidentially destroy the information in accordance with any relevant data retention and disposal policies.

See **Appendix 12** for a checklist to help ensure lawfully sharing of data.

9. Implementation, Monitoring and Review

All of its signatories own the Protocol. This document is an over-arching code of behaviour for all information-sharing applications, supplemented by Information Sharing Agreements (ISAs) for specific purposes. ISAs will adopt the principles and commitments in the Protocol as their base line and identify any additional service specific requirements.

A review of the Protocol will be undertaken every two years and the document updated to account for any changes in legislation and developments in national guidance. Issues arising from breaches of the Protocol, changes in legislation, or recommendations arising from review may result in an earlier review.

Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the Protocol and publishing any individual Information Sharing Agreements they may have.

Any of the signatories can request an extraordinary review at any time when a joint discussion or decision is necessary to tackle local service developments.
Work to develop individual ISAs will be the responsibility of the organisations wishing to share information as will the review of existing ISAs on updates to the Protocol, ISA Template (see **Appendix 14**) and changes to relevant legislation.

10. Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All agencies who are party to this Protocol must have in place appropriate measures to investigate and deal with personal data breaches (both accidental and deliberate). The agency must inform all affected partners of the data breach immediately to enable them, where relevant, to meet their legal duty under UK GDPR to report personal data breaches within 72 hours to the Information Commissioner.

The partner agency where the breach has occurred shall conduct a full investigation of the breach and share the findings with the other relevant partners and the Lancashire Community Safety Partnership Board.

Partners need to record all data breaches in respect of personal data they are Controller in respect of, internally within their organisation and inform the Lancashire Community Safety Partnership Board to ensure effective monitoring and reviews can take place.

See **Appendix 6** for further information.

11. Retention and Disposal

Partners must comply with their own agencies' retention and disposal policies. These should cover both electronic and paper based information.

12. Access to Information and Mutual Assistance

Partners must have in place policies to deal with people's information rights under Freedom of Information (FOI) legislation, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

Each Partner agency shall assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

- Consult with the other partners about any notices given to data subjects in relation to the Shared Personal Data;
- Promptly inform the other partners about the receipt of any data subject access request;
- Provide the other partners with reasonable assistance in complying with any data subject access request;
- Not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the partner from where the information originated, wherever possible;
- Assist the other partner, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with

respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- Notify the other partner without undue delay on becoming aware of any breach of the Data Protection Legislation;
- At the written direction of the Data Discloser, delete or return Shared Personal Data and copies thereof to the Data Discloser on termination of this Protocol unless required by law to store the personal data;
- Use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers;
- Unless impossible or involving disproportionate effort, recipients of information that is subsequently and which is rectified by the respective Controller, will be notified accordingly.
- Maintain complete and accurate records and information to demonstrate its compliance with this clause.

13. Complaints

Partner organisations must have in place procedures to address complaints relating to the inappropriate disclosure of information. The partner organisations agree to cooperate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures and the contact details of the Data Protection Officer (DPO) are well publicised.
If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers/DPOs who should liaise to investigate the complaint.

14. Non Compliance and Partner Disagreement

In the event of a suspected failure within their organisation to comply with this agreement, partner organisations will carry out and record an adequate investigation.

If the partner organisation finds there has been a failure it will ensure that:
- If one partner organisation believes another has failed to comply with this agreement it should notify the other partner organisation in writing giving full details. The other partner organisation should then investigate the alleged failure. If it finds there was a failure, it should take the steps set out above. If it finds there was no failure it should notify the first partner organisation in writing giving its reasons.
- Where it is clear that a partner organisation is not complying with this protocol, other partners may decide to stop sharing information until the issues are resolved.
- More information about information sharing is available **here** from the Information Commissioner.
- Partner organisations will make every effort to resolve disagreements between them about personal information use and sharing. However, they recognise that ultimately each organisation, as Controller, must exercise its own discretion in interpreting and applying this Protocol and ensuring compliance with the data protection legislation.

- Notify nominated representatives at an early stage of any suspected or alleged failures in compliance or partner disagreements relating to their organisation.

15. Protocol Signatories

Signatories to this Protocol have agreed to abide by the terms, appendices and any variations to the Protocol or its appendices. The latest list of signatories is available on Community safety - Lancashire County Council