

**NORTH WEST AND PARTNERS
INFORMATION SHARING CODE OF
PRACTICE**

Information Sharing Protocol

**Pennine Lancashire Community Safety
Partnership**

(Tier 2)

January 2020

1. Introduction

The Pennine **Community Safety Partnership** brings together Blackburn with Darwen, Burnley, Hyndburn and Rossendale Councils, Blackburn with Darwen and East Lancashire NHS Clinical Commissioning Groups, Lancashire Fire and Rescue Service, Lancashire Police and Probation Services, Housing Associations, along with a range of other public and voluntary sector partners.

Public Authorities are often reliant upon an effective information exchange as a key to multi-agency working. The exchange of personal and de-personalised information can be used to:

- Assist strategic planning;
- Help local partnerships to implement the provisions of the Crime and Disorder Act 1998;
- Assist agencies to exchange information, where a power exists to do so in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and in accordance with the precepts of the Human Rights Act;

Advice from the Information Commissioner is that Public Authorities may exchange data provided:

- They have noted their intention to do so;
- That the process of exchange is in accordance with the GDPR and the DPA 2018
- There is a statutory or common law power to do so.

This protocol is to be used as the basis for any information sharing partnership, where it is associated with the requirements of the Community Safety Partnership as outlined in the Crime and Disorder Act (sect 115) as amended by the Police and Justice Act 2006, the Policing and Crime Act 2017, and the Fire and Rescue Services Act (sect 6) 2004.

There is a section which covers the Human Rights Act and specifically some of the articles relevant to information sharing, as well as the principles to consider when deciding whether interference with a convention right is justified.

The protocol will also apply to the exchange of personal information following a conviction by a Court. It will therefore be relevant to:

- Drug Rehabilitation Requirements
- Reparation Orders;
- Action Plan Orders;
- Rehabilitation Activity Requirements
- Post Sentence Supervision
- Detention and Training Orders;
- Parenting Orders;
- Housing eviction Orders.

Finally, the protocol will be applied to any initiative set up for the purposes of protecting life and property, prevention or detection of crime and the maintenance of good order in society.

2. Commitments

The partnership organisations will:

- Ask for permission to collect and share citizen's information, and only do this with their full consent where possible and or for the purposes of preventing and detecting crime (Appendix F). In addition, information collected could be used for the provision of information, publicity and encouragement in respect of the steps to prevent fires and death or injury by fire.
- If explicit consent cannot be obtained then at least one condition from Article 6 of the GDPR must be met and one further condition from Article 9 of the GDPR will also need to be met if the data is regarded as special category personal data.
- Explain why they are using the citizen's information, and will only use it for those purposes.
- Explain who will see it and limit access to the citizen's information only to persons who need it.
- Collect minimum personal and special category information to meet the identified needs of the citizen and not ask for information that is not relevant.
- Record and share citizen's needs with partner organisations as appropriate.
- Keep information about the citizens as accurate and up-to-date as possible – with the citizen's help.
- Respect citizen's rights under the GDPR and DPA 2018 – including the citizen's right to see the information which has been recorded about them.
- Protect citizen's information with the highest standards of security and confidentiality.
- Tell citizens how they can get more information, including:
 - How they safeguard their personal information;
 - How citizens can check and correct any information they hold;
 - How to raise a query or a complaint.
- Only keep the information for as long as needed or as required by statute.

- There may be occasions where information is shared without consent. In such cases, the GDPR and DPA 2018 will apply.

The overarching ambition is for Community Safety Partnership's aims and objectives, to be embedded across all organisations and service providers within the public, voluntary, and community sectors and for information to be used appropriately and legally to facilitate this.

This will require **'collaborative working between service providers and local communities in building the resilience and resourcefulness of residents in Pennine Lancashire'**.

3. Scope

This overarching Protocol sets out the principles for information sharing between Partner Organisations ([Appendix A](#)) and sets out the rules that all people working for or with the Partner Organisations must follow when using and sharing information.

The Protocol applies to the following information:

- All personal information processed by the organisations including electronically (e.g. computer systems, CCTV, Audio etc.), or in manual records.
- Anonymised, including aggregated, personal data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.
- The specific purpose for use and sharing information will be defined in the Data Exchange Agreements that will be specific to the Partner Organisations sharing information.

4. Aims and Objectives

The aim of this Protocol is to provide a framework for the Partner Organisations and to establish and regulate working practices between Partner Organisations. The Protocol also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable 'need to know' purposes

These aims include:

- To guide Partner Organisations on how to share personal information lawfully.
- To explain the security and confidentiality laws and principles of information sharing.
- To increase awareness and understanding of the key issues.
- To support a process, which will monitor and review all data flows
- To encourage flows of data.
- To protect the Partner Organisations from accusations of wrongful use of sensitive personal data.

- To identify the lawful basis for information sharing.

By becoming a Partner to this Protocol, Partner Organisations are making a commitment to:

- Apply all relevant Information Commissioner's Codes of Practice"
- Adhere to or demonstrate a commitment to achieving the appropriate compliance with the current UK Data Protection legislation
- To apply NHS and Social Care Caldicott confidentiality standards where required by law and to consider adopting them as good practice where not required by law.

All Partners will be expected to promote staff awareness of the major requirements of Information Sharing. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partners' Intranet sites and/or via other communication media.

The overarching ambition is for the *Community Safety Partnership's aims and objectives*, to be embedded across all organisations and service providers within the public, voluntary, and community sectors.

Outcomes	Shared outcomes which capture progress in the 'health and well-being' of families and individuals, the protection of residents, businesses and visitors from harm, and a clearer understanding and appreciation of what works.
Assessment	Clear, consistent assessment methodology that links across organisational boundaries, and provides a holistic understanding of our communities needs to include victims and perpetrators of crime and anti-social behaviour.
Information sharing	The ability to prevent and detect crime through the collaborative sharing of information, with systems that track progress alongside a shared understanding of how to support the earliest identification of need and effective management of risk.
Commissioning	Services commissioned and or delivered on the basis of a comprehensive assessment of risk and needs with clearly defined outcomes and evidence of progress and impact.

Families	Services designed in collaboration with communities, victims and perpetrators to enable them to create and sustain their own solutions.
Workforce	<p>Strong collaborative culture where integrated working to achieve solutions to crime and anti-social behaviour is strengthened by the systems and behaviours of the respective organisations.</p> <p>Shared purpose and values for working with communities, and clarity of roles and accountabilities.</p> <p>Clear understanding of what is being delivered, who is delivering it, where it is being delivered and whether it is cost-effective.</p>

This will require collaborative working between families, service providers and local communities in building the resilience and resourcefulness of our communities across Blackburn with Darwen and East Lancashire

This will be considered through a range of key elements as described below:

5. The Legal Framework

The principal legislation concerning the protection and use of personal information is listed below and further explained in [Appendix B](#):

- Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Data Protection Act 2018
- The General Data Protection Regulation

Other legislation may be relevant when sharing specific information. For example, the sharing of information relating to children may involve (but not limited to) consideration of any of the following:

- The Children Act 1989
- The Children Act 2004
- Education Act 2002
- Education Act 1996
- Learning & Skills Act 2000
- Education (SEN) Regulations 2001
- Children (Leaving Care) Act 2000
- Protection of Children Act 1999
- Immigration & Asylum Act 1999
- Local Government Act 2000

- Criminal Justice Act 2002
- Crime and Disorder Act 1998
- Policing and Crime Act 2017
- National Health Service Act 1977
- Health Act 1999
- The Adoption and Children Act 2002
- Mental Capacity Act 2005
- Health and Social Services Act 2000
- 1983 Mental Health Act, as amended by the 2007 Mental Health Act and associated Code of Practice
- Sexual Offences Act 2003
- Police and Criminal Evidence Act 1984
- Fire and Rescue Services Act 2004
- Localism Act 2011

6. Data covered by this Protocol

All personal information and anonymised data (as defined in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)) that is required to facilitate this programme of work is covered by this Protocol. **Anonymous data should be used wherever possible.**

Personal Information

The term 'personal information' refers to **any** information held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that information.

The term is further defined in the GDPR as:

- 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;

The GDPR also defines certain classes of personal information as 'special category data' where additional conditions must be met for that information to be used and disclosed lawfully.

An individual may consider certain information about them to be particularly 'sensitive' and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

All medical and social care data is deemed to be special category personal data and is held under a duty of confidence. Criminal records and allegations of unlawful acts are also deemed special category personal data.

Anonymised Data

Partners must ensure anonymised data, especially when combined with other information from different agencies, **does not** identify an individual, either directly or by summation.

Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed
- The data cannot be combined with any data sources held by a Partner to produce personal identifiable data.

7. Organisational Responsibilities

Each Partner Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.

Partner Organisations will accept the security levels on supplied information and handle the information accordingly.

Partner Organisations accept responsibility for independently or jointly auditing compliance with the Information Sharing Protocols in which they are involved within reasonable time-scales.

It may be better to advise that all employees will undergo DP training to understand the rules around DP and the use of personal and special category information.

Every organisation should ensure that their contracts with external service providers abide by their rules and policies in relation to the protection and use of confidential information.

The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

Partner Organisations should have documented policies for retention, archiving and secure waste destruction.

Partner Organisations should be committed to having procedures in place to ensure the quality of information. It is suggested that they consider having a Data Quality Strategy. A Strategy will secure and ensure the maintenance of good quality standards and identify areas for improvement.

Partner Organisations must be aware that a data subject may with apply their right to object to processing (i.e. article 21 of GDPR) unless an available exemption applies. Where the Partner Organisations rely on consent as the condition for processing then withdrawal means that the condition for processing will no longer apply. Any such withdrawal of consent should be communicated to Partner Organisations and processing cease as soon as possible.

Partner Organisations must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals must be provided with information about these procedures.

8. Indemnity

Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

9. Transparency

All partners will ensure that all personal data is handled lawfully and that all records are handled confidentially.

Lead professionals will provide information to clients and partner organisations only as needed and in a secure manner.

Citizens will be informed at first contact the purpose for collecting and using their data, consent to share that data will also be sought at the first contact with the citizen.

You can view the ***Community Safety Partnership***, privacy notice in [Appendix E](#).

10. Quality and Security of Data

Partner Organisations are committed to maintaining data of the highest quality, quality assurance and audit checks will be carried out by members of the partner organisations to ensure that all partners are maintaining standards and revising data as necessary. Partners will also ensure that any changes to data will be notified to other members quickly and securely.

11. Retention of shared information

Data created for the any purpose on behalf of the '***Community Safety Partnership*** 'will be held in line with each relevant organisation's Records Management policy from the date of creation of the record until the end of the programme. At which time it will be destroyed as confidential data and all partners notified.

12. Security of shared Information

Data will be held securely throughout its life and shared with partners using only secure methods such as email encryption. Each partner will have the right to check that security standards are maintained across partnership members. Security standards are described in tier 1 of this North West Sharing Protocol. Access to shared datasets provided by partner organisations will be permitted on a need to know basis, in line with the requirements of the programme.

13. Access to personal Information

To comply with the rights of the data subject under Article 15 of the GDPR, individuals will have the right of access (subject access request) and to be told whether any personal data is being processed, be given a description of the personal data, the reason for it being processed and given a copy of the information.

Partner Organisations must ensure that only appropriate access to information is granted therefore appropriate procedures must be in place.

If data subjects would like access to their information, then they should apply in writing to the Community Safety Manager for the '**Community Safety Partnership**;

Name: Mark Aspin

Address: Blackburn with Darwen Borough Council, L Floor, Tower Block, Town Hall, BB1 7DY

Contact Details: 01254 585512

The relevant partner organisation(s) are obliged to assist in providing copies of documentation for the Subject Access Request to enable the Data Controller (s) in common to reply to the request within 1 calendar month. The data controller(s) in common must also inform the partner organisation group of any such request.

14. Review

This protocol will be reviewed every two years.

15. Complaints

Each organisation will be required to handle complaints in accordance with their own organisation's procedure. The partner organisation leads must also be informed of any such complaints.

16. Non Compliance and Partner Disagreement

In the event of a suspected failure within their organisation to comply with this agreement, Partner Organisations will ensure that an adequate investigation is carried out and recorded.

If the Partner Organisation finds there has been a failure it will ensure that:

- necessary remedial action is taken promptly;
- service-users affected by the failure are notified of it, the likely consequences, and any remedial action;
- Partner Organisations affected by the failure are notified of it, the likely consequences, and any remedial action.

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.

Partner Organisations will make every effort to resolve disagreements between them about personal information use and sharing. When doing so they should refer to the Tiered Agreements and Associated Documents. However, they recognise that ultimately each organisation must exercise its own discretion in interpreting and applying this Agreement in line with guidance from the Information Commissioner.

Partner organisations will make every effort to resolve disagreements between them about personal information use, recording and sharing. Ultimately each organisation must exercise its own discretion in interpreting and applying this protocol in line with guidance from the Information Commissioner

Nominated representatives should ensure they are notified at an early stage of any suspected or alleged failures in compliance or partner disagreements relating to their Partner Organisation.

17. Appendices

Appendix A: List of lead officers involved in agreeing this protocol

Appendix B: The Legal Context


Appendix C: Glossary


Appendix D: Meeting Confidentiality Statement


Appendix E: Fair Processing Notice

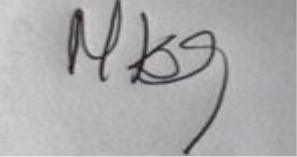
18. Signatures


In signing this document partners are signing to accept the whole of this agreement, including tiers zero and one and agree to the principles supporting them.

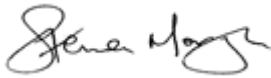
Signed For and on Behalf Of BWDBC	
Name; SAYYED OSMAN	
Position; Director of Adults & Prevention (DASS), Adults, Communities and Prevention	
Date; 04th February 2020	


Signed on behalf of Lancashire Constabulary	
Name; ANDREA BARROW	
Position; Superintendent	
Date; 12th February 2020	


Signed on behalf of Blackburn with Darwen & East Clinical Commissioning Group	
Name; KIRSTY HOLLIS	
Position; Chief Finance Officer (EL CCG) and SIRO For EL & BwD CCG	
Date; 16th April 2020	


Signed For and on Behalf of National Probation Service	
Name; MARY KELLY	
Position; Acting Head of South East Lancashire Cluster	
Date; 05th February 2020	


Signed for and on Behalf of Together Housing Group	
Name; KEVIN RUTH	
Position; Deputy Group Chief Executive	
Date; 04th February 2020	

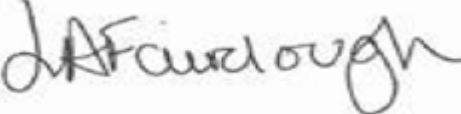
Signed For and on Behalf Of Lancashire Fire and Rescue	
Name; STEVEN MORGAN	
Position; Head of Service Delivery	
Date; 18th February 2020	

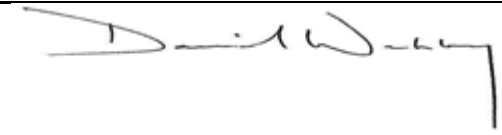
Signed For and on Behalf of Lancashire County Council	
Name; LAURA SALES	
Position; Director of Corporate Services	
Date; 06th February 2020	

Signed on behalf of Burnley Borough Council	
Name; MICK CARTLEDGE	
Position; Chief Operating Officer	
Date; 04th February 2020	

Signed For and on Behalf of Rossendale Borough Council	
Name; NEIL SHAW	
Position; Chief Executive	
Date; 13th February 2020	

Signed on behalf of Lancashire & Cumbria Rehabilitation Company	
Name: JOANNE DANN	
Position; Deputy Director	
Date; 04th February 2020	

Signed For and on Behalf of The Office of the Police & Crime Commissioner for Lancashire	
Name; LOUISE FAIRCLOUGH	
Position; Victims & Vulnerable People Lead	
Date; 18th February 2020	

Signed on behalf of Hyndburn Borough Council	
Name: DAVID WELSBY	
Position; Chief Executive Officer	
Date; 20th February 2020	

Appendix (B)

LEGAL CONTEXT

THE GENERAL DATA PROTECTION REGULATION / THE DATA PROTECTION ACT 208.

Data Protection legislation governs the standards for the processing of personal data including the collection, use of and disclosure of such information. The legislation requires that data controllers meet certain obligations. It also give individuals or 'data subjects' certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the six data protection principles summarised as follows:

Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- b) 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, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) 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');
- e) 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 in accordance with [Article 89\(1\)](#) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- f) 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').

THE HUMAN RIGHTS ACT 1998

The UK Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

Where the disclosure of data has the potential for breaching an individual's human rights,

Disclosure must be for a lawful purpose, be for a reason specified in the Act, be necessary, proportionate and the minimum possible to achieve the intended aim.

Article 8 of the Act states that:

“Everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law”. It is likely that this exchange of information will be for the purposes of one of the following legitimate aims:

- In the interests of national security.
- Public Safety.
- Economic wellbeing of the country.
- The prevention of crime and disorder.
- The protection of health or morals.
- The protection of the rights or freedoms of others.

FREEDOM OF INFORMATION ACT 2000

Information held by or on behalf of a public authority may be disclosed to a party requesting it except where a statutory exemption applies. For example, personal data is normally exempt under the Act (but may be disclosable under GDPR); as is information provided under a duty of confidence.

LOCAL GOVERNMENT ACT

The main power specific to local authorities is section 2 Local Government Act 2000 – the power of "well-being". This enables LA's to do "anything" to promote social, economic, or social well-being in their area provided the act is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out the act it gives regard to its own community strategy. For example, all councils are taking measures, including data sharing, to reduce crime in its area in order to promote well-being. In addition S111 Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place. The above are general powers available to local authorities. In addition, authorities are granted statutory powers relating to specific activities and these should be referred to as appropriate in the Data Exchange Agreement.

LOCALISM ACT 2011

A relevant fire and rescue authority may do—

(1)(a) Anything it considers appropriate for the purposes of the carrying-out of any of its functions (its “functional purposes”),

(b) Anything it considers appropriate for purposes incidental to its functional purposes,

(c) Anything it considers appropriate for purposes indirectly incidental to its functional purposes through any number of removes,

(d) Anything it considers to be connected with—

(i) Any of its functions, or

(ii) Anything it may do under paragraph (a), (b) or (c), and

(e) For a commercial purpose anything which it may do under any of paragraphs (a) to (d) otherwise than for a commercial purpose.

(2) A relevant fire and rescue authority’s power under subsection (1) is in addition to, and is not limited by, the other powers of the authority

POLICE ACT 1996

The Police Act 1996 gives a Constable certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff. In addition, the Code of Practice on the Management of Police Information 2005 defines the policing purpose as:-

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

The policing purpose set out in the Code does not replace or supersede any existing duty or power defined by statute or common law. In addition, this does not define every

Policing activity and does not mean that there is no legal basis for performing such activities. For example, roads policing, public order, counter-terrorism or protection of children or other vulnerable groups while not referred to explicitly are non the less legitimate policing functions.

THE CRIME AND DISORDER ACT 1998

Section 115 of the Crime and Disorder Act 1998 confers a power on any ‘relevant authority’ (which are the police, local authority, Clinical Commissioning Group and probation services or to any other person acting on behalf of such authority)

to exchange that information which is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder. The parties to this exchange agreement are relevant authorities for the purposes of this legislation.

Section 17 Crime and Disorder Act 1998 requires that all Local Authorities consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the Crime and Disorder Act impose a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area.

FIRE AND RESCUE SERVICES ACT 2004

Section 6 of the Fire Services Act requires that all Fire and Rescue Authorities must make provision for the purpose of promoting fire safety in its area.

In making provision under subsection (1) a fire and rescue authority must in particular, to the extent that it considers it reasonable to do so, make arrangements for:

- (a) The provision of information, publicity and encouragement in respect of the steps to be taken to prevent fires and death or injury by fire.
- (b) The giving of advice, on request, about:
 - (i) How to prevent fires and restrict their spread in buildings and other property;
 - (ii) The means of escape from buildings and other property in case of fire.

COMMON LAW DUTY OF CONFIDENTIALITY

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are generally three categories of exception to the duty of confidence:

- Where there is a legal compulsion to disclose.
- Where there is an overriding duty to the public.
- Where the individual to whom the information relates consented.

Partners should consider which of these conditions are the most relevant ones for the purposes of this exchange agreement. The guidance from the Information Commissioner states that because such decisions to disclose 'in the public interest' involves the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions. The partners to this agreement should document within this agreement how this duty will be maintained, e.g. need to know.

SUB JUDICE

Information obtained during a criminal investigation and any subsequent proceedings must not be disclosed where to do so would risk prejudice to the investigation or subsequent proceedings. Disclosure of data which creates a substantial risk that the course of justice in the proceedings in question will be

seriously impeded or prejudiced is a criminal offence (Contempt of Courts Act 1981).

CALDICOTT

Where Health Data is concerned; when sharing information with others, due regard must be given to the Caldicott principles listed below. Ensure that all the conditions are met before sending the data. If unsure then speak to your line manager, or the appropriate Caldicott Guardian.

Caldicott Principles:

- Justify the purpose before sharing information.
- Only use patient identifiable data when absolutely necessary.
- Use the minimum that is required, do not share more data than is necessary, i.e. do not send the whole patient record when only the request relates to a recent event.
- Access to the data should be on a strict need to know basis.
- Be aware of your responsibilities in complying with organisational policies relating to confidentiality
- Understand the law, if uncertain, speak to you line manager.

Where Health Data is concerned Health staff, and others working in partnership with them, should be aware of the concept of Safe Haven.

Safe Havens will:

- Provide a secure location restricting access to only authorised staff and will be locked outside normal hours.
- Be staffed by those individuals with authority to access confidential information and who are under contractual and statutory obligations to maintain confidentiality
- Ensure that no confidential information will be released to parties outside a Health Trust unless it is deemed appropriate. Health Staff should make reference to the Caldicott Principles listed above and seek advice from the Caldicott guardian where uncertain.
- Ensure that wherever possible the NHS number is present and person identifiable data has been removed.

Appendix C - Glossary of Terms

Accessible Record – unstructured personal information usually in manual form relating to health, education, social work and housing.

Agent – acts on behalf of the data subject.

Aggregated – collated information in a tabular format.

Anonymous data – anonymous data is where an Organisation does not have the means to identify an individual from the data they hold. If the Data controller has information, which allows the Data Subject to be identified, regardless of whether or not they intend to identify the individual is immaterial - in the eyes of the IC this is not anonymous data. Data Controller must be able to justify why and how the data is no longer personal.

CCTV – close circuit television.

Consent – The GDPR defines the conditions for consent within Article 7 <https://gdpr-info.eu/art-7-gdpr/> as “a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement”

Data/Information –

a) Information being processed by means of equipment operating automatically or

b) Information recorded with the intention it be processed by such equipment.

c) Recorded as part of a relevant filing system or

d) Not in a or b or c, but forming part of an accessible record.

e) Recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller – a person or a legal body such as a business or public authority who jointly or alone determines the purposes for which personal data is processed.

Data Flows – the movement of information internally and externally, both within and between organisations.

Data Processing – any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Processor – operates on behalf of the Data Controller. Not staff.

Data Set – a defined group of information

Data Subject – an individual who is the subject of personal information.

Disclosure – the passing of information from the Data Controller to another organisation / individual

Duty of Confidentiality – everyone has a duty under common law to safeguard personal information.

European Economic Area (EEA) – this consists of the twenty eight EU members together with Iceland, Liechtenstein and Norway.

Fair processing – to inform the Data Subject how the data is to be processed before processing occurs

Health Professional – "health professional" means any of the following who is registered as:

A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor, and osteopaths. *And* Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960

currently extends to, clinical psychologists, child psychotherapists and speech therapist, music therapist employed by a health service body, and scientist employed by such a body as head of department.

Health Record – any information relating to health, produced by a health professional.

Need to know – to access and supply the minimum amount of information required for the defined purpose.

Personal Data – means data relating to a living individual who can be identified from those data (including opinion and expression of intention).

Processing – any operation performed on data. Main examples are collect, retain, use, disclosure and deletion.

Purpose – the use / reason for which information is stored or processed.

Recipient – anyone who receives personal information for the purpose of specific inquiries

Relevant Filing System – two levels of structure,

(i) Filing system structured by some criteria

(ii) Each file structured so that particular information is readily accessible.

Special Category Personal Data – The GDPR defines sensitive personal data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Serious Crime – There is no absolute definition of "serious" crime, but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences". These include:

- Murder
- Manslaughter
- Rape
- Kidnapping
- Certain sexual offences
- Causing an explosion
- Certain firearms offences
- Taking of hostages
- Hijacking
- Causing death by reckless driving
- Offences under prevention of terrorism legislation

Subject Access – the individual's right to obtain a copy of information held about themselves.

Third Party – any person who is not the data subject, the data controller, the data processor (includes Health, Housing, Education, Carers, Voluntary Sector etc. as well as members of the public).

Appendix D - Confidentiality Statement

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the General Data Protection Regulation, the Data Protection Act 2018, the Human Rights Act 1998 and the common law duty of confidentiality, all attendees are asked to agree to the following. This agreement will be recorded in the minutes.

1. Information can be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.
2. A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the subjects' confidentiality and a breach of the confidentiality of the agencies involved.
3. All documents exchanged should be marked 'Restricted – not to be disclosed without consent'. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.
4. If further action is identified, the agency (ies) who will proceed with this action(s) should then make formal requests to any other agencies holding such personal information as may be required to progress this action quoting their legal basis for requesting such information. Information exchanged during the course of this meeting must not be used for such action.
5. If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting and a decision will be made on the lawfulness of the disclosure such as the prevention or detection of crime, apprehension or prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

This confidentiality agreement is in relation to the **Community Safety Partnership, Programme.**

Signature.....Date.....

Name.....

Representing Organisation.....

.....

Copies of this signed agreement are to be held by the Chair

Appendix E

PRIVACY NOTICE

Community Safety Partnership,

Pennine Lancashire

What is Personal Data?

Under the General Data Protection Regulation (GDPR), Personal Data is defined as 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;

Personal data will therefore cover basic details such as name, address, telephone number, and Date of Birth, in fact any data from which you can be identified.

Why does Community Safety Partnership, need to collect personal data?

In order to provide you with a service, lead professionals from a range of different organisations need to collect personal data for correspondence purposes and detailed service provision. In any event the organisations are committed to ensuring that the information they collect and use is 'Fit for Purpose', and does not constitute any invasion of your privacy. They may pass your personal data on to our service providers who are committed to Community Safety Partnership, in the course of providing you with a service.

Our providers are obliged to keep your details securely, use them only to fulfil your service request and be compliant with the Data Protection Act. Once your service need has been satisfied or your case has been closed, they will dispose of the details in line with their organisational procedures. If the lead professional needs to pass your personal data on to a third party they will only do so once they have obtained your consent, unless we are legally required to do so.

How we will use your Information

Community Safety Partnership, will collect, store and use the information you provide in a manner that is compliant with the General Data Protection regulation and the Data Protection Act 2018. Lead professionals will try to keep your information accurate and up to date and not keep it for longer than is necessary, but you will need to inform us of any changes to your personal details. In some instances the law sets the length of time information has to be kept, but in other cases they will ensure that they do not keep records any longer than needed to provide a service to you.

Our aim is not to be intrusive, and lead professionals will not ask irrelevant or

unnecessary questions. Any information you provide will be subject to security systems and procedures which minimise the risk of unauthorised access or disclosure.

The Community Safety Partnership Programme in Blackburn with Darwen

Blackburn with Darwen Council has committed to the Government to deliver the national programme in our area. In order to fulfil our obligations it is necessary to share information with critical partners. This is not only in delivering the programme but also in evaluating its effectiveness.

In order to identify families, understand the difference we are making and focus on who can potentially access the additional support the programme offers we will be sharing personal records that relate to you.

This data will be shared for research purposes with the Department for Communities and Local Government and the Office of National Statistics. The data included in this research relates to people/families that were assessed for the programme along with those who have participated in the programme.

This might include records in relation to your social care, any involvement with the police, courts and probation, aspects relating to your employment, anti-social behaviour, violence in the home, substance misuse, educational attendance and behaviour, vulnerable children and health issues.

The personal data of individuals and families will be linked with information from public agencies. Organisations such as the NHS and health organisations, Department of works and pension, the Police, the ministry of Justice, the probation services, schools and Youth offending Team. The reason to link the information is to help the government and local service providers understand whether or not the programme has been effective in reducing offending, truancy and getting people ready for work and to help improve the service over time.

Data agreements are in place to ensure that:

- The data can only be used for carrying out research;
- The linked data cannot be used to make decisions about individuals;
- The linked information is anonymised to reduce the risk of individuals being identified;
- It will be impossible for any person or family to be identified from any published reports;
- The linked personal data will not be shared with or made available to the local authority or any other public agency;
- All data is transferred, handled and stored in accordance with the Data Protection Act;
- Appropriate measures are in place to prevent unauthorised use of the data;
- The data is destroyed after five years.

Using Your Personal Data

Lead professionals will use the information you provide for the following purposes where appropriate:

- To provide you with the support they discuss with you as part of the Community Safety Partnership, process
- This may involve sharing your data with partner organisations but we will seek your consent wherever appropriate before we do this.

Partnership working

Community Safety Partnership, is serious about delivering appropriate and effective services – it is important to us that we co-ordinate what we do for you properly.

Over time we aim to have one master record containing your basic details, together with information about the nature of your involvement with Community Safety Partnership. The database will not be designed to provide in depth details of the services you have received - but rather to ensure that we are not asking you to repeat basic information for each service you require. It will also help us to tailor our services to meet your needs, and ensure that your requests are being dealt with.

Your Rights

We will not use your information for third party marketing purposes, or pass it on to third parties, other than those who either process information on our behalf or because of a legal requirement.

You have the right to ask the Council for personal information held about you. Details of how to do this can be found here;

<https://www.blackburn.gov.uk/data-and-information/personal-information-and-data-protection/personal-information-request>

You may also ask the Council to consider any objections you may have to the processing of your personal information, including processing for research purposes.

For more details please contact the Community Safety Partnership, Project Manager on 01254 585512.

Changed to this Privacy Notice

Blackburn with Darwen Council may amend this Privacy Notice from time to time. If we make any substantial changes in the way we use your personal information we will make that information available by amending this notice.

