Children and Adults Safeguarding

Overarching Tier 1 Data Sharing Agreement

for Pan-Lancashire partners

December 2025

General:

Date Tier 1 DSA comes into force:	
Last review:	December 2025
Date for review of DSA:	2 years from ratification
DSA Owner (Organisation):	Lancashire County Council
DSA Author(s):	Lancashire Safeguarding Business Unit

Version control:

Version	Date	Author	Edit/Update
0.1	February 2024	Lancashire Safeguarding Business Unit: Vaishali Bamania & Medina Patel	Input from DfE appointed experts from Somerset Council and NHS England
0.2	November 2024	Lancashire Safeguarding Business Unit: Vaishali Bamania & Medina Patel	Consultation with partners.
0.3	October 2025	Lancashire Safeguarding Business Unit: Hannah Taylor	Consultation with partners.
0.4	November 2025	Lancashire Safeguarding Business Unit: Hannah Taylor & Medina Patel	Partner sign off
Final	December 2025	Lancashire Safeguarding Business Unit: Hannah Taylor & Medina Patel	Board ratification

1. Contents

2 Introduction

To make informed decisions about safeguarding and achieve quality outcomes for individuals, we must share information with our partner agencies who also have responsibilities for safeguarding and prevention.

Effective safeguarding often depends on timely and appropriate information sharing between agencies. Past reviews have shown that failing to share information can lead to serious harm or even loss of life. A fear of sharing sensitive information must not be a blocker to safeguarding and promoting the welfare of children and adults at risk. This agreement aims to prevent such outcomes by making clear when and how information should be shared.

The relevant UK government departments and independent non-departmental government bodies responsible for protecting children and/or regulating data protection set out policy, legislation, and statutory guidance on how the protection system should work and data protection compliance is achieved at the same time.

These pieces of legislation provide the foundation for safe, legal, and effective information sharing between safeguarding partners. It enables them to understand their responsibilities and the legal framework, which ensures information is shared lawfully, proportionately, and when necessary to protect children and adults at risk.

Information and data have increasingly been used in the same context and are used interchangeably in this agreement.

This is a high-level, strategic agreement that sets out the principles and framework for how different organisations (such as local authorities, NHS bodies, police, probation, and others) will share information in relation to Child and Adult Safeguarding.

The agreement:

- Identifies what types of data can be shared (e.g., personal and special category data relevant to safeguarding).
- Describes the situations (“contexts”) in which sharing is appropriate (such as responding to safeguarding concerns or facilitating early intervention).
- Lists the organisations (“parties”) involved and their roles in making these decisions.
- References the legislation and legal justifications that allow or require information sharing (such as the Children Act 2004, Care Act 2014, UK GDPR, and Data Protection Act 2018).

The partners of this agreement are aware and understand their legal responsibilities to deliver safeguarding to the whole population as defined (amongst others) in the statutes listed at Appendix 3:

The effective and timely sharing of information between agencies and organisations is essential to enable early intervention and preventative work for safeguarding and promoting welfare of those experiencing and at risk of abuse and harm and for wider public protection. For this reason, this Tier 1 Data Sharing Agreement (DSA) applies to all areas of children’s and adult safeguarding. In the context of this document a Tier 1 DSA can be understood as an overarching, strategic agreement between Safeguarding partners defining the appropriate arrangements to support multi-organisational information sharing for safeguarding reasons.

3 Signatories

The organisations below are signatories to this Tier 1 Data Sharing Agreement (see Appendix 5 for further details):

Organisation(s)
Blackburn with Darwen Borough Council
Blackpool Council
Blackpool Teaching Hospital
East Lancashire Hospital Trust
HCRG Care Group
Lancashire Constabulary
Lancashire County Council
Lancashire Fire and Rescue Service
Lancashire & South Cumbria Foundation Trust
Lancashire Teaching Hospital Trust
Mersey West Lancashire Care Group
National Probation Service
NHS Lancashire and South Cumbria Integrated Care Board (ICB)
Northwest Ambulance Service
University Hospitals of Morecambe Bay NHS Trust
Other strategic partners that have responsibilities to address issues relevant to safeguarding children and adults

4 Scope

This Tier 1 Data Sharing Agreement applies to organisations operating across Pan-Lancashire is a multi-agency agreement between Local Authorities, NHS Organisations, the Integrated Care Board, Police, Probation, Prison Service and Voluntary Sector Organisations. A full list of signatory organisations can be found under section 3 Signatories and in Appendix 5.

The Agreement covers the sharing of personal and special category data about children, young people, and adults for safeguarding reasons. This agreement is not contractually or legally binding but is setting good practice standards that the sharing partners are required to meet.

The Lancashire Children Safeguarding Assurance Partnership, Blackpool Multi Agency Safeguarding Arrangements, Blackburn with Darwen Safeguarding Children Partnership, Lancashire Safeguarding Adults Board, Blackpool Safeguarding Adults Board and Blackburn with Darwen Safeguarding Adults Board is constituted to deliver relevant statutory duties as follows:

- To safeguard and promote the welfare of children as required by The Children Act 2004 and supported by the statutory guidance, Working Together to Safeguard Children 2023.
- To cooperate to improve the wellbeing of children and young people as defined in The Children Act 2004.
- To help and protect adults with care and support needs at risk of abuse or neglect as defined by the Care Act 2014 and supporting statutory guidance.

The responsibility for joined up working in safeguarding rests locally with safeguarding partners who have a shared and equal duty to make arrangements to work together to safeguard children and adults in a local area. These partners are:

a) The Local Authorities
b) Integrated Care Board (ICB)
c) Police

The safeguarding partners should agree ways to co-ordinate their safeguarding services, act as a strategic leadership group in supporting and engaging others; and implement local and national learning including from serious child/adult safeguarding incidents/learning reviews.

In safeguarding adults, the Care Act statutory guidance states the following about lead agency and wider partner involvement:

- 14.137 Safeguarding requires collaboration between partners in order to create a framework of inter-agency arrangements. Local authorities and their relevant partners must collaborate and work together as set out in the co-operation duties in the Care Act and, in doing so, must, where appropriate, also consider the wishes and feelings of the adult on whose behalf they are working.
- 14.138 Local authorities may cooperate with any other body they consider appropriate where it is relevant to their care and support functions. The lead agency with responsibility for coordinating adult safeguarding arrangements is the local authority, but all the members of the SAB should designate a lead officer. Other agencies should also consider the benefits of having a lead for adult safeguarding.

The Care Quality Commission (CQC) describes safeguarding as protecting people's health, wellbeing, and human rights, and enabling them to live free from harm, abuse and neglect. It's fundamental to high-quality health and social care.

The Department for Health and Social Care provides guidance on the Care Act 2014 through the 'Care and support statutory guidance' and describes adult safeguarding as 'an adult's right to live in safety, free from abuse and neglect. It is about people and organisations working together to prevent and stop both the risk and experience of abuse or neglect…'.

The Care Act 2014 states that safeguarding duties apply to an adult aged over 18 who:

- has needs for care and support (whether or not the authority is meeting any of those needs) and
- is experiencing, or is at risk of, abuse or neglect, and
- as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

The Department for Education defines children's safeguarding within their 'Working Together to Safeguard Children 2023' guide to inter-agency working to safeguard and promote the welfare of children:

- providing help and support to meet the needs of children as soon as problems emerge.
- protecting children from maltreatment, whether that is within or outside the home, including online.
- preventing impairment of children's mental and physical health or development.
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care.
- promoting the upbringing of children with their birth parents, or otherwise their family network through a kinship care arrangement, whenever possible and where this is in the best interests of the children.
- taking action to enable all children to have the best outcomes in line with the outcomes set out in the Children's Social Care National Framework.

The Information Commissioner's Office (ICO) recognises in their 10-step guide to sharing information to safeguard children that there is no single definition of safeguarding but highlights the inclusion of

- preventing harm;
- promoting the welfare of a child; and
- identifying risk in order to prevent harm (especially helpful where the risk may not be obvious to a single person or organisation).

Safeguarding must therefore be seen as a protection of wellbeing (including physical, mental & emotional); a prevention of harm and reduction of risk through care and support requiring information sharing. This allows intervention in immediate situations demanding the safeguarding of children and adults but also sharing for prevention and early intervention in less immediate or high-risk situations.

This DSA is for use by professionals, staff and volunteers of organisations who have signed, and therefore agreed to the terms of this agreement and providers of services commissioned by the organisations who have signed this agreement. Safeguarding is everyone's responsibility, not just safeguarding practitioners.

Where there needs to be a more specific agreement about sharing data, it will be necessary to complete a Tier 2 Data Sharing Agreement. This agreement should not be seen as an alternative to a Tier 2 agreements which must be completed for specific information sharing projects between the partner organisations but will be linked to this overarching agreement.

The Tier 2 agreement should be developed in line with best practice and/or using the National Template and Guidance provided by the Department for Education which can be found here (Data Sharing Agreements – Important information for professionals (somerset.gov.uk)).

Whilst tier 2 agreements will address specific data sharing requirements, parties should seek to recognise and differentiate between the immediate safeguarding scenario and requests and those which can be considered in slower time.

Information sharing with non-statutory agencies e.g. charities is within the scope of this Tier 1 DSA. There are a number of charitable organisations that offer support and services. Such organisations are not created under statute and therefore do not have statutory powers; nevertheless, they are often able to offer help and provide assistance in the form of counselling, advice, support and guidance as well as referring individuals to other organisations and charities within their network.

Adults in custodial settings are outside of the scope of this agreement e.g., prisons and similar approved premises. Prison Services have responsibility under the common law duty of care to protect those in their custody. Local Authorities however have a duty to assist prison services on adult safeguarding matters.

5 Purpose and benefits

The purpose of this Tier 1 Safeguarding DSA is to facilitate the lawful sharing, use and security of personal, special category data and criminal offence data in order to safeguard both children and adults who require safeguarding intervention and to facilitate the statutory functions of the Childrens Safeguarding Partnerships and Safeguarding Adult Boards (SABs).

This agreement will function as the foundation to embed strong, effective multi-agency arrangements that are responsive to local circumstances and engage the right people. Signatories to this agreement must be engaged to work in a collaborative way to provide targeted support as appropriate. This approach will provide flexibility to enable joint identification of, and response to, existing and emerging needs, and to agree priorities to improve outcomes.

This agreement provides an overall framework for the secure sharing of information between organisations (multi-agency/integrated working) who are parties to this agreement with the intention of:

- Protecting people's health, wellbeing, and human rights, and enabling them to live free from harm, abuse and neglect (including self-neglect).
- Taking action to enable all children and adults to have the best outcomes.
- Identifying risk and emerging threats in order to prevent harm (prevention, early intervention).
- Raising public awareness so that communities as a whole, alongside professionals, play their part in preventing, identifying and responding to abuse and neglect and promoting the welfare of children and adults.
- Preventing impairment of children's mental and physical health or development.
- Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care.
- Safeguarding adults in a way that supports them in making choices and having control about how they want to live (in line with the Mental Capacity Act 2005).
- Providing information and support in accessible ways to help people understand the different types of abuse, how to stay safe and what to do to raise a concern about the safety or well-being of an adult.
- Collaborating, sharing and co-owning the vision for how to achieve improved outcomes for vulnerable children and adults.
- Challenging appropriately and holding one another to account effectively.
- Sharing information effectively to facilitate more accurate and timely decision making for children and adults.
- Ensuring that shared learning is promoted and embedded in a way that local services for children, families and adults can become more reflective and that changes to practice are implemented.
- Reducing the need for individuals to provide duplicate information when receiving an integrated service.
- Managing risks, performance, service planning and auditing.
- Fulfilling all the statutory safeguarding obligations set out in guidance – Working Together to Safeguard Children (2023) and Chapter 14 Care Act Guidance

6 Responsibilities / partner commitments

By becoming a partner to this sharing agreement all organisations are making the following commitments. It is understood that signatories to this agreement are committing their entire organisation to entirely support the principles and carry out their responsibilities to the full.

Area of responsibility:
The parties to this DSA are committed to ensuring that information is shared appropriately between those professionals/organisations working with children and adults at risk of harm across Pan-Lancashire and who have a legitimate need for that information to assist with delivering a high quality, integrated safeguarding service that meets the needs of the relevant individuals.
Organisations signed up to this agreement commit to sharing confidential information in accordance with their legal, statutory, and common law duties and meet the requirements of any additional supporting guidance.
All organisations must have in place policies and procedures to comply with Data Protection law, and which are consistent with this DSA. The existence of, and adherence to, such policies provide all organisations with confidence that data shared will be transferred, received, used, held and disposed of appropriately.
The parties acknowledge their 'Duty of Confidentiality' to the people whose data they hold. In requesting or considering the release and disclosure of personal information from other organisations, the parties recognise that only in circumstances where there is a significant public interest, e.g. safeguarding, can this common law duty be set aside. In such circumstances clear evidence must be provided to the recipient articulating the overriding public interest and/ or the legal gateways being relied upon. This responsibility also extends to third party disclosures; any proposed subsequent re-use of data which is sourced from another organisation should be approved by the source organisation.
Where processing is likely to result in a high risk to the rights and freedoms of a natural person (as per UK GDPR, Article 35), a Data Protection Impact Assessment (DPIA) will need to be completed and shared with the relevant partners as appropriate. This agreement does not replace the need to conduct a DPIA of the information or processes involved.
An individual's personal information must be complete and up to date and will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes, data should be anonymised.
Where it is agreed that the sharing of personal information is necessary, only that which is needed, relevant and appropriate will be shared and would only be on a 'need to know' basis.
When disclosing information about an individual; organisations will clearly state whether the information being shared is fact, opinion, or a combination of the two.

Area of responsibility:
There will be occasions where it is legal and / or necessary for organisations to request that personal information supplied by them is kept confidential from the person concerned. Decisions must be linked to a detrimental effect on the physical or mental wellbeing or safety of that individual or other parties involved with that individual. The outcome of such requests and the reasons for taking such decisions will be recorded.
All organisations agree to make reasonable efforts to ensure that recipients of personal information are kept informed of any changes to the information that they have received, so that records can be kept up to date.
Careful consideration will be given to the disclosure of personal information concerning a deceased person, and if necessary, further advice should be sought before such data is released to maintain the duty of confidentiality still owed to the deceased.
All organisations will ensure that Subject Access Requests and other Individual Rights requests made to them are responded to in accordance with the requirements outlined in the UK General Data Protection Regulation (UK GDPR)Carl Melling: and Data Protection Act (2018).
All organisations agree that appropriate annual/regular training will be given to staff so that they are aware of their responsibilities to ensure personal information is processed lawfully.
All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.
Organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of personal information.
Extreme care and careful consideration should be taken where the disclosure of information includes third party information and particularly personal data relating to witnesses, victims or complainants.
The person or persons to whom a request is made must comply with such a request in relation to a child death review or child safeguarding practice review, Domestic Homicide Reviews (DHRs) or Safeguarding Adult Reviews (SAR) and if they do not do so, the safeguarding partners may take legal action against them.

7 Lawfulness

Partners agree that in order to share personal data, there needs to be a relevant legal gateway. It is important to note that the existence of this Tier 1 Safeguarding Data Sharing Agreement does not provide partners with a legal gateway or secure an automatic right or obligation to share information with or from another partner. This may come from statue, common law, or legal precedent.

Statutory powers (also referred to as legal gateways) will differ between the signatory organisations and cannot be prescribed in this Agreement. A list of commonly used legal gateways / applicable legislation for sharing safeguarding information, by signatory organisations is noted in Appendix 3.

Principle legislation governing the protection and use of personal information is:

a. UK General Data Protection Regulation (GDPR) 2016
b. Data Protection Act (DPA) 2018
c. Data (Use and Access) Act 2025
d. Human Rights Act 1998 (article 8)
e. The Common Law Duty of Confidentiality

Each signatory must be able to identify their lawful basis to share personal data which should be recorded within a Tier 2 Data Sharing Agreement and the DPIAs. The lawful basis under the UK GDPR and Data Protection Act 2018 is however likely to be the following:

Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.

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

Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

Article 9(2)(g) – processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

A relevant condition from Schedule 1 of the Data Protection Act 2018 will be identified as appropriate in relation to each purpose. Where the processing of criminal conviction or offence information is undertaken for a non-law enforcement purpose, a suitable condition from Schedule 1,2 or 3 of the Data protection Act 2018 will be identified.

Where sharing by the Police is for one of the law enforcement purposes the sharing will fall under the scope of Part 3 of the Data Protection Act 2018, with the Police acting as a competent authority.

Where the sharing is necessary for General purposes, the Police will be required to consider Section 36(4) of the DPA 2018 which limits the processing of Part 3 personal data for the UK GDPR purposes unless ‘authorised by law’. Such authorisation may derive from statute, Common Law or Statutory Code. Authorisation may be provided for example by the Police Act 1996 or the Counter Terrorism and Security Act 2015, as well as the Statutory Code relating to Police Information and Records Management 2023.

8 Security Standards

Each partner will be responsible for ensuring data is subject to sufficient security.

All partners signed up to this agreement must ensure appropriate organisational policies and procedures are in place to cover the security of personal information under this agreement.

All reasonable steps should be taken to ensure that confidentiality of data is maintained, the integrity of data is preserved and that data remains available where needed.

Partners must also consider determining how they will test/audit the effectiveness of information security controls as part of a Data Protection Impact Assessment (DPIA).

Sharing arrangements involving shared systems/assets will require joint decisions on security controls, therefore responsibility may be shared (pertinent to joint controller arrangements). This may include (but is not limited to) decisions on:

- A satisfactory level of compliance with industry cyber/information security standards (e.g. Cyber Essentials) and/or Quality Assurance standards e.g. ISO 27001
- A role-based access model
- Patching schedules
- Remote access solutions
- Third party security assurances and contractual arrangements (which may permit certain autonomy to maintain security)
- Recovery point/time objectives

It may be applicable to complete a version of the DSPT where there are different versions depending on the size and type of organisation. The Data Security and Protection Toolkit (DSPT) is something which will be relevant for health care organisations and local authorities; however the police have their own standards they adhere to. Organisations should work towards an equivalent standard depending on the type of organisation and the level of data being processed, and it is recommended that they attain cyber essentials certification (Cyber Essentials – NCSC.GOV.UK)

A system level security policy should be developed jointly for such assets to document the agreed security controls/assurances for the sharing partners and demonstrate controller responsibility.

Appropriate contractual, data processing and confidentiality agreements must be in place to underpin the processing of personal information by a third party / processor.

9 Consent

The signatories of this agreement understand that 'Consent is considered one lawful basis for sharing, but it is not required for sharing information in a safeguarding context. In fact, in most safeguarding scenarios you will be able to find a more appropriate lawful basis.' (Source ICO).

The UK GDPR provides several bases for sharing personal information. Partners will however be transparent with individuals whose data is being processed if it does not increase the risk of harm. The difference between consent to treatment/service opt-in and consent to share information under Data Protection laws must be understood by all partners to this agreement. If consent to share information is considered to be required, this must be escalated to the relevant partner organisation's Data Protection Officer (DPO) for review.

Best practice in respect of transparency is to take a layered approach by utilising various methods to communicate information about how individuals' data is being used, i.e., website privacy notice, leaflets, posters, letters, conversations, etc., However, given the nature of processing for safeguarding purposes it may not always be appropriate. The sharing partners must consider exemptions (e.g., law enforcement purposes under Part 3 of the DPA 2018, or serious harm to the physical or mental health of any individual).

Each organisation must be clear, open, and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'. The sharing partners (controllers) each have a responsibility to take reasonable steps to ensure that individuals (to whom data they are processing pertains) are informed of the uses of their data. The sharing partners will therefore follow their own agency guidelines and processes pertaining to informing individuals about the sharing of data for safeguarding purposes. The privacy information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language, tailored to children if required.

10 Proportionality and necessity

The data relevant under this Tier 1 Data Sharing Agreement can include personal data, special category data and criminal offence data shared for the reasons of safeguarding.

Partners agree that only information that is relevant to the purposes should be shared with those partners who need it (need to know basis). Assessing proportionality and necessity for any sharing initiative under this agreement is paramount and should be documented to assure compliance with current UK data protection legislation. In circumstances where data is to be shared for safeguarding purposes both the benefits and the risks must be balanced against each other to assure the right level of proportionality and necessity.

Organisations signed up to this Tier 1 Data Sharing Agreement must therefore include Caldicott Guardians (for Health), Service Leads or other equivalent individuals as they must be core to such decision-making. It is recommended under this agreement that organisations take a default 'starting position' of considering what data/information is reasonably, foreseeably needed. Data minimisation and proportionality will be maintained by only asking for data that is needed to fulfil a specified purpose.

Partners must consider any harm or detriment that may come from sharing information, and make sure this does not outweigh what is trying to be achieved (least intrusive amount of personal information to be shared appropriate to the risk presented). This is particularly important for sensitive information. Partners will consider who could be affected by any disclosures contemplating that sharing information about one individual may also have an effect on the privacy rights of others. Information must be of the right quality to ensure that it can be understood and relied upon.

Organisations signed up to this agreement will consider the level of identification required for each sharing initiative.

11 Retention

Records will be retained and disposed of in accordance with data protection legislation and national and local/organisational guidelines. Each organisation which has received information referred to in this agreement has to follow their own Retention and Disposal Policy which should state how long they will keep different types of information. Additionally, organisations should consider the business need beyond any national/industry code or guidance which could justify a shorter or longer retention period. Retention periods should be agreed with sharing partners, at the early stages of data sharing, in a Tier 2 Data Sharing Agreements as relevant (documented justification). Especially sharing arrangements involving shared systems/assets require joint decisions on retention and/or system configuration as they are more complex.

Health and Social Care partners will consider the NHS England Health and Social Care Records Management Code of Practice (revised) 2023 to inform decision making. The Constabulary (and other Police Forces) must consider and also comply with the statutory College of Policing Management of Police Information (MoPI) Code of Practice relating to Police and Information Records Management, and associated Guidelines, (also known as the Authorised Professional Practice (APP)) for Police Information. Other partners will consult the relevant industry guidelines.

National inquiries must be considered when assessing records for destruction.

Any records which no longer need to be retained in accordance with the partner's own policies and procedures should be destroyed under secure conditions.

12 Individuals' Rights

The partners agree that in simple sharing arrangements each Controller will handle subject rights requests in accordance with their own established processes and policies. In multi-stakeholder sharing arrangements where shared information assets/systems are used, responsibilities for the handling of individuals' rights requests by the sharing partners must be clearly set out in the relevant Tier 2 Data Sharing Agreement.

Requests relating to information shared for safeguarding purposes are likely to require careful consideration and may require assistance from partners as the provider of the information may be aware of a wider context to make a fully informed decision. Therefore, sharing partners agree to set out clear arrangements in a Tier 2 Data Sharing Agreement or Policy for the handling of individuals' rights and provide reasonable assistance to sharing partners as required.

The right to be informed – Partners must ensure that individuals are informed about the collection and use of their personal data and are provided with the privacy information required as per current data protection law. See the following section 'Transparency' for further detail.

The right of access – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate requests, what the process shall be if a request is received by them but is relevant to another organisation, how partners' involvement affects what they should disclose and the process for determining lawful reasons to withhold data from disclosure (i.e. if they are viewing data in a shared asset but are not controller nor a joint controller of the data, or if they are a joint controller).

The right to object and the right to restrict – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate objections and restriction requests, what the process shall be if an objection or restriction request is received by them but is relevant to another organisation and the process for determining whether to uphold the objection or restriction request (although unlikely due to the nature of processing).

The right to rectification – Sharing partners will agree a process of how to respond to requests for rectification (i.e. if received by them but it is relevant to another organisation). The process will be dependent upon the sharing arrangement this may require action from multiple partners (especially when a request for rectification of a professional opinion is received) or by a single partner that has provided the data into a shared asset and may require partners to assist each other to determine whether data should be rectified.

The right to erasure - Sharing partners will agree a process of how to respond to requests for erasure (i.e. if received by them but it is relevant to another organisation). It is unlikely to uphold a request for erasure when processing for Safeguarding reasons.

Automated decision-making and profiling – If the sharing arrangement is to involve automated decision-making or profiling then the sharing partners will agree how individuals affected will be informed of this (unless an exemption applies) and how requests for a member of staff to review any such activity will be handled. As it stands, data used for safeguarding purposes is unlikely to be classed as 'automated decision making' or 'profiling' without human intervention prior to decisions being made that affect individuals.

The right to data portability – If the sharing arrangement is to involve the processing of data based on the explicit consent of the data subject or a contract with the data subject (which are both highly unlikely for the purposes of safeguarding), or data will be carried out by automated means, then the sharing partners shall ensure that it is possible for data to be provided to the data subject in a structured, commonly used and machine-readable format and/or have this data transmitted to another controller. The lawful basis of processing data for safeguarding purposes is not likely to be explicit consent. Therefore, it is unlikely that the right to data portability applies.

Any Information Rights request directed at the *Pan Lancashire Partnership* should be forwarded to the relevant business unit to coordinate the appropriate response. When a partner agency requires cooperation from the Partnership to respond to a Subject Access Request they should contact the relevant Business Support Team Manager to ensure appropriate liaison.

13 Transparency

Each organisation must be clear, open and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'. The sharing partners (controllers) each have a responsibility to take reasonable steps to ensure that individuals (to whom data they are processing pertains) are informed of the uses of their data.

The sharing partners will therefore follow their own agency guidelines and processes pertaining to informing individuals about the sharing of data for safeguarding purposes. This may, for example, take the form of each partner updating their own privacy information (i.e., a website privacy notice) or the partners may agree to reference a single privacy notice from their own privacy information, which is then maintained by one or several organisations (e.g., joint controllers where the parties share a common purpose for the processing and information sharing). The privacy information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language, tailored to children if required.

Best practice in respect of transparency is to take a layered approach by utilising various methods to communicate information about how individuals' data is being used, i.e., website privacy notice, leaflets, posters, letters, conversations, etc., However, given the nature of processing for safeguarding purposes it may not always be appropriate. The sharing partners must consider exemptions (e.g., law enforcement purposes under Part 3 of the DPA 2018, or serious harm to the physical or mental health of any individual).

As required by the Data Protection Act 2018, it is the responsibility of each organisation to consider and publish an Appropriate Policy Document should they process special category personal data or criminal offence data, when relying on the relevant processing conditions that require such.

Each organisation should also consider any transparency obligations, both to individuals and to partner organisations, relating to their use of AI systems and follow their own Acceptable Usage Policies, SOPs and guidance to ensure compliance.

14 Staff development

Each sharing partner must ensure that its staff are sufficiently trained to handle personal data appropriately as part of their controller responsibilities under UK data protection law (the UK GDPR principle of 'accountability' and specifically principle 5(f) (integrity and confidentiality) as an appropriate organisational measure). This can include training on confidentiality, data protection, record keeping, records management, system training, as well as more specific training on handling individuals' rights requests for those staff typically involved in these, etc.

Sharing partners should therefore consider whether staff affected by a new sharing arrangement will require additional training (in addition, controllers should continually assess the training needs of their workforce, which is often done by maintaining/appraising a 'Training Need Analysis' on a routine basis as set out in the annual DSPT).

All staff must have access to the policies of their own organisation, this agreement and any materials jointly developed. For the purposes of this agreement the supporting processes will be that all staff authorised to access information will be trained in the basic requirements of the Data Protection legislation and have an awareness of the implications associated with shared information. They will also understand the risks associated with inappropriate disclosures and the impact that this has on safeguarding and the necessity to undertake thorough checks.

Staff contracts must therefore contain appropriate confidentiality clauses detailing the possible consequences of unauthorised or inappropriate disclosure of personal information. Each organisation must have in place disciplinary procedures to be invoked if a member of staff is found to have breached the confidentiality of an individual. Consideration should be given to the category and nature of information to which staff have access and whether their role includes any specific requirements to access personal information.

The process of supervision is generally confidential between the supervisor and supervisee(s). The ground rules in relation to confidentiality will be made explicit, such as ownership of supervision records, retention of information. There may be occasions when it is necessary to share information with other practitioners/ managers/ external agencies/professional bodies in the best interests of the child at risk in line with organisational and multi-organisational Data Sharing Agreements. Poor or dangerous practice will be addressed in line with partner organisation policy and procedures.

The partners of this agreement will work together to jointly develop staff training materials to allow organisations to this agreement to incorporate the principles of this agreement. Resources can be found in appendix 4.

15 Incident Management and Complaints

Data security and protection incidents must be treated with priority and urgency; swift action should be taken to contain incidents and prevent both the number of individuals that may be affected and increased severity for those already affected. As such, all partners must have an Incident Management Policy and supporting procedures and act in accordance with them.

Sharing partners must also determine whether other sharing partners (beyond those responsible) should be informed as concerns may have been, or be, raised to them that are linked to the incident, which they may otherwise not know. The partner organisation where the incident has occurred should lead on the assessment and reporting, including, if the incident is considered serious enough, informing the ICO.

Given the nature of the data involved in processing for safeguarding purposes, care and consideration should be given to who needs to be informed of an incident (in terms of both sharing partners, as well as the individuals affected and/or third parties and the organisation's Caldicott Guardian as per an organisation's own information governance process).

Where an incident is isolated and deemed to only affect one sharing partner then the incident may be handled solely by that sharing partner according to their own incident management policy and processes. Where multiple sharing partners are affected, they must be prepared to establish a joint incident response plan. Clear responsibilities should be set out for any joint controller arrangements.

Complaint handling should follow a similar path; however, they are unlikely to require such priority/urgency unless they are intrinsically linked to an incident. Organisations must ensure that they comply with requirements of the Data (Use And Access) Act in relation to complaints, and seek to follow guidance issues by the Information Commissioner.

All partner organisations must put in place processes that allow concerns about non-compliance with this agreement to be reported to the designated person.

16 Common sharing initiatives / area of work

The below sharing initiatives are covered by this agreement and give detail of how data is being used to safeguard children and their families, and adults at risk.

Child Death Reviews

Multi-agency partners share information through the Joint Agency Review process (for unexpected deaths of children) and subsequent Child Death Review to learn from child deaths. Information is submitted through eCDOP and coordinated by the Pan Lancashire Child Death Overview Panel. Partners provide information about their involvement with the child and their wider family and the child's death.

Child Death Overview Panel (CDOP)

The Child Death Overview Panel (CDOP) is a group of multi-agency professionals who meet four times a year to carry out an independent review of deaths of children in their area. The purpose of the panel is to learn lessons and share any findings which may help to prevent future deaths. The panel will consider and identify any issues relating to the death which may be relevant to the welfare of children in that area or to public health and safety.

They will consider if action should be taken in relation to the issues identified to help try to prevent similar deaths happening again in the future. For the panel to investigate a child's death essential information needs to be gathered including demographic data, and information relating to the circumstances of death and background medical history. Whilst not all deaths reported to the coroner proceed to inquest (although most unexplained deaths of children do) there is also a duty on professionals to disclose such information to the coroner in an un-redacted format and the coroner has their own common law and statutory powers to enforce such disclosure.

For the purposes of the Children Safeguarding Partnerships we share information with the CDOP under Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject and Schedule 1 of the Data Protection Act 2018 Article 9(2)(g) Substantial Public Interest for statutory and government purposes, and for safeguarding of children and individuals at risk.

Multi Agency Safeguarding Hub (MASH), CADS and Request for Support (RfS) - Children and Adults

The goal of a MASH (Multi Agency Safeguarding Hub), and RfS is to improve safeguarding and promote the welfare of children and young people and adults through the timely exchange of proportionate and accurate information following an enquiry by any professional or member of the public. The MASH, and RfS environment is unique in the way it enables multiple sources of information to be considered and shared in a secure and safe location. For Children information is referred to the First Response service and the MASH, or RfS process is triggered. This assists decision making about the threshold of concern and what level of support is required form agencies.

Safeguarding Practice Reviews – Children and Adults

Safeguarding Adult Reviews

A Safeguarding Adult Review (SAR) is a process conducted when an adult at risk has died or suffered serious harm, and there are concerns about the care or services they received. The Safeguarding Adults Boards conduct SARs in line with the Care Act (2014) and aims to identify areas for improvement in policies, procedures, and practice, and to inform training and development for professionals. In undertaking these we aim to prevent similar incidents in the future. Sharing the right information, at the right time, with the right people is fundamental to good practice in safeguarding adults.

When undertaking a SAR the Safeguarding Adults Boards collect and share personal information which includes the name, date of birth and addresses of individuals that are pertain to the SAR and request information and records from professionals who have worked with adults including health records, social care files and criminal records. This information is shared with partners who are involved in review's learning panel and/or agencies' safeguarding leads. The information requests are centrally held and coordinated by the Safeguarding Business Units. The information will be shared with an Independent Reviewer where they have been commissioned. The final reports will be shared with relevant partners and published.

Child Safeguarding Practice Reviews

Children's Safeguarding Partnerships have a statutory responsibility to undertake rapid reviews and Local Child Safeguarding Practice Reviews (CSPRs) where abuse or neglect of a child is known or suspected, and the child has died or been seriously harmed. The purpose of a Child Safeguarding Practice Review is to establish whether there are lessons to be learnt from the case about the way in which local professionals and organisations work together to safeguard and promote the welfare of children. Identify clearly what those lessons are, how they will be acted on, and what is expected to change as a result, and therefore, improve inter-agency working and better safeguard and promote the welfare of children.

When undertaking a review or CSPR, Childrens Safeguarding Partnerships collect and share personal information which includes the name, date of birth and addresses of individuals that are pertain to the CSPR and request information and records from professionals who have worked with children and families including health records, social care files and criminal records. This information is shared with partners who are involved in review's learning panel and/or agencies' safeguarding leads. The information requests are centrally held and coordinated by the Safeguarding Business Units. The information will be shared with an Independent Reviewer where they have been commissioned. The final reports will be shared with the National CSPR Panel, OFSTED and the Department of Education as well as other inspectorates where required such as the CQC and HMIC.

Local Learning Reviews/Multi Agency Reflective Reviews (MARRs)

Children's Safeguarding and Adults Safeguarding Partnerships undertake local learning reviews or MARRs where a referral has not met the criteria for a Rapid Review/SAR. The purpose of a local learning review or MARR is to establish whether there are lessons to be learnt from the case about the way in which local professionals and organisations work together to safeguard and promote the welfare of children/adults. They identify clearly what those lessons are, how they will

be acted on, and what is expected to change as a result, and therefore, improve inter-agency working and better safeguard and promote the welfare of children.

When undertaking a local learning review or MARR, Childrens Safeguarding Partnerships and Safeguarding Adults Boards collect and share personal information which includes the name, date of birth and addresses of individuals that are pertain to the review and request information and records from professionals who have worked with children, adults and families including health records, social care files and criminal records.

This information is shared with partners who are involved in review's learning panel and/or agencies' safeguarding leads. The information requests are centrally held and coordinated by the Safeguarding Business Units. The final reports will be shared with the local Children Safeguarding Partnership Board/Safeguarding Adults Board.

Section 47 (Children Act 1989)

Children's social care have a duty under Section 47 of the Act to make enquiries where there is reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm. These enquiries may be undertaken as a single agency or jointly with police and/or health professionals. Children's social care will seek relevant information from other professionals about the child, their wider family, and/or individuals who may pose a risk to them or be responsible for their care. Information will be provided through strategy meetings, in verbal and/or written communication, through observations and joint visits to children and families, and through automated information sharing electronic systems.

Section 17 (Children Act 1989)

Information is requested by agencies involved in working with children and their families where they are being assessed or are receiving a services as child in need. This is to enable the agencies to provide services which meet the children's identified needs in order to keep them safe from neglect or physical, emotional or mental harm, or to protect their physical, mental, or emotional well-being. Information will be shared verbally between professionals in meetings and communication, in writing and through automated information sharing systems such as Think Family Database, CPIS and Connecting Care.

Section 42 of the Care Act - Adults

Organisations share information with each other to:

- prevent death or serious harm.
- coordinate effective and efficient responses.
- enable early interventions to prevent the escalation of risk.
- prevent abuse and harm that may increase the need for care and support.
- reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse.

- identify low-level concerns that may reveal people at risk of abuse.
- protect adults with care and support needs from organisations and people in positives of trust.
- help people to access the right kind of support to reduce risk and promote wellbeing.
- help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour.
- reduce risk of organisational abuse or neglect.

This will be done primarily through referrals to the adult safeguarding teams who will coordinate information sharing across the multi-agency partnership through telephone calls, emails and multi-agency meetings.

Quality Assurance, Inspection and Scrutiny

The Children Safeguarding Partnerships, Safeguarding Adults Boards and Local Authorities have a requirement to quality assure the effectiveness of children and adult safeguarding. To do this the Safeguarding Business Units will coordinate the sharing of information in the form of reports, data, audit reports and peer reviews and inspections to enable the analysis of quality and performance of systems. This could include sharing personal information of individuals particularly in the case of quality assurance activity. Where this is the case a specific review team will undertake assurance of that area of practice. Steps will be taken to ensure that personalised information is protected in the sharing of learning for example in scrutiny reports or in Children Safeguarding Partnerships and SABs annual reports.

LADO and allegations against professionals

The LADO (Local Authority Designated Officer) is a local authority role who is responsible for ensuring that children are protected from abuse and/or neglect by people in positions of trust (professionals and volunteers). The LADO provides advice and guidance to other professionals and helps determine how allegations should be investigated and managed. The LADO will receive information by a referral form. T

he LADO helps co-ordinate information sharing also monitors and tracks any investigation with the expectation that it is resolved as quickly as possible. The LADO will provide advice and guidance to organisations, regulators, inspectorates, and individuals. They will review HR reports and investigations material which could include CCTV, body maps, statements from staff, observation charts. Each Local Authority LADO will provide anonymised data to their own local Children Safeguarding Partnership about the effectiveness of allegations management in their Local Authority.

PiPoT

"People in a Position of Trust" are those "that work, in either in a paid or unpaid capacity, with adults with care and support needs" (Care and support statutory guidance).

The Care Act 2014 requires the local authority's relevant partners, and those providing universal care and support services, to have clear policies in place for dealing with allegations against anyone working in a position of trust, and also places a requirement on the Safeguarding Adults Board to establish a framework for how allegations should be notified and responded to, ensuring the clear distinction between an allegation, a concern about the quality of care or practice or a complaint.

It should be noted that the above list is not exhaustive, and some of these examples might be subject to specific tier 2 data sharing agreements, but any data sharing for Safeguarding Children/Adults purposes will still fall under this agreement where there is a clear, understood and justified purpose for data sharing and when it is safe, legal and appropriate to do so.

There is a duty on Local Authorities under the Children and Families Act 2014 and the Care Act 2014 to assure a safe transition from Children's to Adult Services. Where there are ongoing safeguarding concerns or needs for a young person and it is anticipated that on reaching 18 years of age, they are likely to require adult safeguarding support, the relevant arrangements should be discussed as part of the transition and the appropriate information must be shared.

17 Dissemination, monitoring and review of the agreement

This Agreement will be shared with all signatories, processors and relevant parties for the purpose of upholding the principles contained within.

It is intended that this overarching Tier 1 Data Sharing Agreement contains high level principles and partner commitments only. It will therefore be reviewed every two years to establish if the sharing remains necessary, still operates as intended and, has or is, achieving the intended benefits, unless legislative changes or other significant changes require immediate action. The monitoring and review of this protocol will be undertaken by:

- Lancashire Childrens Safeguarding Assurance Partnership
- Blackpool Multi-Agency Safeguarding Arrangements
- Blackburn with Darwen Safeguarding Children Partnership
- Lancashire Safeguarding Adults Board
- Blackpool Safeguarding Adults Board
- Blackburn with Darwen Safeguarding Adults Board
- Lancashire Constabulary

Subject to there being no significant changes, the Agreement may be extended on an annual basis without seeking further approval or new signatures. However, any significant changes will require the full approval process.

In the event that this Tier 1 Agreement is not renewed or is otherwise withdrawn, it is incumbent on the parties to amend their records accordingly and to communicate the status of the agreement within their respective organisations to interested parties and the wider public as necessary. The obligations of confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

19 Signatories

Each organisation should identify who is the most appropriate post holder within their agency to sign the DSA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their agency/organisation to the agreement. Additionally, each agency will be asked to identify the post which is responsible on a day-to -day basis for monitoring compliance with this DSA.

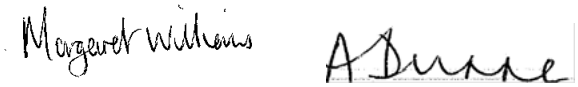
By signing this DSA, all signatories acknowledge and accept the requirements placed upon them and others within their organisations by the DSA and their responsibilities under data protection legislation. A decision needs to be made if the signatory is a list of organisations all signing one document in turn, or if a single organisational signature is collected per copy of the DSA, with a central point of collection and maintained list of signatories.

1. Signed on behalf of:
Name: Lancashire County Council
Role: Data Protection Officer
Email: joanne.winston@lancashire.gov.uk
Signature: 
Date signed: 17/09/2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Medina Patel, Senior Business Manager, Lancashire Safeguarding Business Unit

2. Signed on behalf of:
Name: Blackpool Council
Role: Data Protection Officer
Email: Jonathan.Pickup@blackpool.gov.uk
Signature: 
Date signed: 17/11/2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Sarah Hargreaves and Sarah Rahmat, Business Managers, Blackpool Business Unit

3. Signed on behalf of:
Name: Blackburn with Darwen Borough Council
Role: Data Protection Officer
Email: sarah.critchley@blackburn.gov.uk
Signature: 
Date signed: 10/11/2025

Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Abdul Aziz-Ghiwala,

4. Signed on behalf of:
Name: NHS Lancashire and South Cumbria ICB
Role: Director(s) of Safeguarding
Email: Margaret.williams11@nhs.net / ann.dunne2@nhs.net
Signature: 
Date signed: 01.04.2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: SPOC, Lscicb.safeguarding@nhs.net

5. Signed on behalf of:
Name: Lancashire Constabulary
Role: Assistant Chief Constable – Crime & Vulnerability
Email: Mark.Winstanley@lancashire.police.uk
Signature: 
Date signed: 29/11/2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Carl Melling – Head of Data Protection

6. Signed on behalf of:
Name: Blackpool Teaching Hospital
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

7. Signed on behalf of:
Name: East Lancashire Hospital Trust
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

8. Signed on behalf of:
Name: Lancashire Teaching Hospital Trust
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

9. Signed on behalf of:
Name: Lancashire and South Cumbria Foundation Trust
Role: Head of Safeguarding
Email: jo.morrison@lscft.nhs.uk
Signature: 
Date signed: 06/11/25
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Michelle Brammah, Head of Data Protection

10. Signed on behalf of:
Name: Southport and Ormskirk Hospital Trust
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

11. Signed on behalf of:
Name: HCRG Care Group
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

12. Signed on behalf of:
Name: University Hospitals of Morecambe Bay NHS Trust
Role:
Email:
Signature:
Date signed:
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA:

13. Signed on behalf of:
Name: Probation Service
Role: Head of Central Lancashire Probation Delivery Unit
Email: elaine.seed@justice.gov.uk
Signature: E Seed
Date signed: 28/03/2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Kevin.Kelly1@justice.gov.uk

14. Signed on behalf of:
Name: Lancashire Fire and Rescue Service
Role: Prevention Manager
Email: Liamwilson@lancsfirerescue.org.uk
Signature: 
Date signed: 14th April 2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Robert Shaw - Knowledge and Information Officer

15. Signed on behalf of:
Name: Northwest Ambulance Service
Role: Named Professional for Safeguarding Adults and Children
Email: Jane.Whittaker@nwas.nhs.uk
Signature: *Jane Whittaker*
Date signed: 15/09/2025
Person/Post responsible on a day-to-day basis for monitoring compliance with this DSA: Joanne Moran – Information Governance Manager

Appendix 1 - Glossary of terms

Term	Definition
Ad-hoc data sharing	Information sharing outside a formal meeting or system, often on a one-off basis.
Appropriate Policy Document (APD)	An appropriate policy document is a short document outlining your compliance measures and retention policies. It is required under the Data Protection Act 2018 for some of the conditions documented in Schedule 1 (Part 1, 2 and 3).
Caldicott Guardian	A senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian. Further, guidance has been issued under the Health and Social Care (National Data Guardian) Act 2018 that recommends "other organisations providing services as part of the publicly funded health service, adult social care, or adult carer support" should have a Caldicott Guardian by 30/06/2023: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf
Common law duty of confidentiality	The common law duty of confidentiality is not codified; it is based on previous judgements in court. Whilst various interpretations of the common law may be possible it is widely accepted that, where information which identifies individual service users is provided and held in confidence, disclosure may only be justified in one of three ways: 1. the service user has given consent for their information to be used; 2. the balance of public and private interest favours public interest disclosure; or 3. a statutory basis exists which permits or requires disclosure. (source: Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016, Explanatory Note, Common Law Duty of Confidentiality)
Consent	Consent under Data Protection Law is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Criminal Offence Data	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.

Term	Definition
Data	The use of data in this document must be understood as information which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Data Controller / Joint Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Protection Act (DPA) 2018	The DPA 2018 sits alongside and supplements the UK GDPR.
Data Protection Impact Assessment (DPIA)	A process to help you identify and minimise the data protection risks related to processing of personal data. A DPIA is legally required in some circumstances.
Data Protection Officer (DPO)	The primary role of the data protection officer (DPO) is to ensure that their organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
Data Subject	The individual to whom the data being processed relates and is identified/identifiable by that data.
Data Sharing	Data sharing as used within this document can be understood as sharing of personal data.
Data Sharing Agreement (DSA)	Terminology can vary (Data Sharing Protocol, Data Sharing Contract, Personal Data Sharing Agreement) but can be used interchangeably in the guidance. A DSA can be used between sharing partners (Controllers) to help demonstrate compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality and other relevant laws. It should help you justify your data sharing, clarify responsibilities of the sharing partners and set agreed parameters for the use of data.
European Economic Area (EEA)	The EEA includes EU countries and Iceland, Liechtenstein, and Norway. The UK has adequacy regulations in place about these countries (expected to last until 27 June 2025).
Information	The use of information in this document must be understood as organised data providing context which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Immediate Safeguarding	Where there is a risk to the life/ or immediate serious harm or danger to the well-being of a child or adult.
Information Commissioner's Office (ICO)	The UK's independent body set up to uphold information rights.

Term	Definition
Law Enforcement Processing	Processing (including sharing) of personal data by competent authorities (for definition click here) for a Law Enforcement Purpose.
Law Enforcement Purposes	As defined by Section 31 Data Protection Act 2018 - the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (for details click here).
Legal gateway	Legislation and common law that establishes justifiable grounds for the processing of personal data.
Local Authority (LA)	An LA is a local government organisation responsible for the administration of government policy at a local level.
Means [of processing]	Actions taken in the processing of data to achieve the purpose(s) for its processing i.e. how the data is processed but can also be considered to extend to what data is used to achieve the purpose(s).
Multi-Agency Safeguarding Hub (MASH)	The Multi-Agency Safeguarding Hub (MASH) brings key professionals together to facilitate early, better quality information sharing, analysis, and decision-making, to safeguard vulnerable children and young people more effectively.
Personal data	Data that relates to a living identified or identifiable individual.
Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Purpose(s) [of processing]	Reasons to process personal data.
Secure File Transfer Protocol (SFTP)	A protocol for securely accessing and transferring large files across the web.
Special Category Data	Data pertaining to an identified or identifiable individual that reveals their 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.
Tier 1 DSA	In this document Tier 1 Data Sharing Agreement can be understood as an overarching Multi Agency Safeguarding Data Sharing Agreement which can be used by all agencies and organisations within the relevant geographical area to provide a framework for data sharing between the partners. Sometimes Tier 1 Agreements are referred to as: Overarching DSA, Data Sharing Protocol, Data Sharing Charter, and others.

Term	Definition
Tier 2 DSA	In this document a Tier 2 Data Sharing Agreement can be understood as a more operational document setting out the purpose of data sharing for a specific initiative, detailing what happens to the data at each stage, setting specific standards and helping all the parties involved in sharing to be clear about their roles and responsibilities.
UK Data Protection Legislation	For the purpose of this template/guidance the UK data protection legislation means the UK GDPR and the DPA 2018 and regulations made under the DPA 2018 which apply to a party relating to the use of personal data.
UK General Data Protection Regulation (GDPR)	Legislation that determines lawful and unlawful use of individuals' data, and places requirements on those processing data, to ensure appropriate use and adequate protections.

Appendix 2 - Information sharing checklist (routine/formalised sharing)

By sharing information, we work better together, and this Tier 1 Safeguarding Data Sharing Agreement encourages the appropriate sharing of personal information between the relevant agencies. If you cannot identify an individual from the information you are planning to share, then you are free to share. However, if the information identifies someone, please use this checklist to help you determine that it is safe to share information. Here is a simple checklist of what you will need to do to go from having concerns about sharing data to sharing data legally and securely with confidence.

Why is the information needed?

What is the purpose for sharing the relevant information, think about the purpose for individuals, your organisation and the wider public.

What information is needed?

Be specific and descriptive, consider how often it is required.

What organisation can provide the information?

Have you explored if the information is available already, maybe in other parts of your organisation. Have you spoken to a counterpart in the potential sharing organisation who can advise you on what information is available and how often.

Have you completed a Data Protection Impact Assessment (DPIA)?

Be aware that a DPIA is likely to be a legal requirement for routine sharing. Complete it before you start processing any data.

How will it be transferred?

Consider your options and assess the risk of those. Transfers must be safe and secure, consult with your technical teams for more complex digital solutions (e.g., data transfer system to system or via Secure File Transfer Protocol [SFTP]).

Where will it be held?

Consider your options and assess the risk of those. Any information must be held safe and secure, consult with your technical teams for more complex digital solutions.

Are you sure the information is accurate and not misleading?

Take all reasonable steps to ensure the personal data you hold is not incorrect or misleading. If you discover that personal data is incorrect or misleading, you must take steps to correct or erase it as soon as possible. Carefully consider any challenges to the accuracy of personal data.

How will you process it?

Define what solutions are available to process the information (e.g., data warehouse, modelling, risk scoring, manual usage to inform cases), work closely with the relevant teams (e.g., analytics, IT, ethics).

How long will you keep it?

Follow your internal retention policy and establish how long you need the information. Include any potential outcome products and long-term requirements to hold the data.

How will you delete the data?

Follow your internal records retention or data destruction policy to assure safe destruction of the information you hold. Consider the method depending on your storage solution to allow for safety of destruction.

Appendix 3 - Applicable Legislation & Guidance

Legislation:

Children Act 2004, Section 10

Each local authority must make arrangements to promote co-operation between partners (including the ICB, Police, Schools and others) to improve the well-being of children including:

(a)physical and mental health and emotional well-being.

(b)protection from harm and neglect.

(c)education, training, and recreation.

(d)the contribution made by them to society.

(e)social and economic well-being.

Children Act 2004, Section 16H

(1)Any of the safeguarding partners for a local authority area in England may, for the purpose of enabling or assisting the performance of functions conferred by section 16E *[Local arrangements for safeguarding and promoting welfare of children]* or 16F *[Local child safeguarding practice reviews]*, request a person or body to provide information specified in the request to
(a)the safeguarding partner or any other safeguarding partner for the area,

(b)any of the relevant agencies for the area,

(c)a reviewer, or

(d)another person or body specified in the request.

(2)The person or body to whom a request under this section is made must comply with the request.
(3)The safeguarding partner that made the request may enforce the duty under subsection (2) against the person or body by making an application to the High Court or the county court for an injunction.
(4)The information may be used by the person or body to whom it is provided only for the purpose mentioned in subsection (1).

Working Together to Safeguard Children 2023

This guidance is under:

- Section 7 of the Local Authority Social Services Act 1970, which requires local authorities in their social services functions to act under the general guidance of the Secretary of State
- Section 27 of Children Act 1989 which requires agencies to co-operate with the local authority to safeguard children
- Section 47 of the Children Act 1989 which requires agencies to co-operate with the local authority to undertake child protection enquiries
- Section 10(8) of the Children Act 2004, which requires each person or organisation to which the section 10 duty applies to have regard to any guidance given to them by the Secretary of State

- Section 11(4) of the Children Act 2004 which requires each person or organisation to which the section 11 duty applies to have regard to any guidance given to them by the Secretary of State
- Section 16B(7) of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that the Child Safeguarding Practice Review Panel must have regard to any guidance given by the Secretary of State in connection with its functions
- Section 16C(2) of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that local authorities must have regard to any guidance given by the Secretary of State in connection with their functions relating to notifications
- Section 16K of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that safeguarding partners and relevant agencies for a local authority area in England must have regard to any guidance given by the Secretary of State in connection with their functions under sections 16E to 16J of the Act 10
- Section 16Q of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that the child death review partners for a local authority area in England must have regard to any guidance given by the Secretary of State in connection with their functions under sections 16M to 16P of the Act
- Section 175(4) of the Education Act 2002, which states that governing bodies of maintained schools (including maintained nursery schools), further education institutions and management committees of pupil referral units must have regard to any guidance given by the Secretary of State
- Paragraph 7(b) of the Schedule to the Education (Independent School Standards) Regulations 2014, made under sections 94(1) and (2) of the Education and Skills Act 2008, which states that the arrangements to safeguard or promote the welfare of pupils made by the proprietors of independent schools (including academies or free schools) or alternative provision academies must have regard to any guidance given by the Secretary of State
- Paragraph 3 of the Schedule to the Non-Maintained Special Schools (England) Regulations 2015, made under section 342 of the Education Act 1996, which requires arrangements for safeguarding and promoting the health, safety, and welfare of pupils in non-maintained special schools to have regard to any guidance published on such issues

Care Act 2014, Section 1

Duty on Local Authorities to promote an individual's well-being including:
(a)personal dignity (including treatment of the individual with respect).

(b)physical and mental health and emotional well-being.

(c)protection from abuse and neglect.

(d)control by the individual over day-to-day life (including over care and support, or support, provided to the individual and the way in which it is provided);

(e)participation in work, education, training, or recreation.

(f)social and economic well-being.

(g)domestic, family and personal relationships.

(h)suitability of living accommodation.

(i)the individual's contribution to society.

Care Act 2014, Section 6

Duty for the local authority and agencies that undertake care and support services for adults, including their carers, to share information with each other to undertake their functions as set out in the Act.

Care Act 2014, Section 42

Section 42 which requires agencies to co-operate with the local authority to undertake adult safeguarding enquiries

Care Act 2014, Section 45

Requirement for any agency to supply information to a Safeguarding Adult Board (SAB) so that the SAB can undertake its functions

Information Sharing: advice for practitioners providing safeguarding services

This advice outlines the importance of sharing information about children, young people and their families in order to safeguard children. It should be ready alongside the statutory guidance Working Together to safeguard children 2023.

In addition to the legal obligations on safeguarding laid out above, all parties to this agreement must follow and abide by the following:

The Eight Caldicott Principles

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations between individuals, both for individual care and for other purposes.

Records Management Code of Practice

Provides guidance on how to keep records, including how long to keep different records.

Confidentiality: NHS Code of Practice

Provides guidance to the NHS and NHS related organisations on patient information confidentiality issues.

Data Protection Act 2018

The UK GDPR sets out seven key principles which should lie at the heart of the partnership's approach to processing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Please visit the ICO website for more detail on the principles.

Common Law Duty of Confidentiality (CLDC)

Common law is not written out in one document like an Act of Parliament (Statute). It is a form of law based on previous court cases decided by Judges (i.e. based on precedent).

Health and care providers are able to share patient data for the purposes of direct care without breaching confidentiality. When considering sharing patient data for non-direct care/secondary purposes such as planning or research, the CLDC needs to be set aside to avoid breaching confidentiality.

When processing individual information for secondary purposes, compliance with the common law is achieved when one of the following circumstances applies:

i)Individuals have provided their Explicit Consent; or

ii)There is a statutory or other legal requirement; or

iii)The public interest served by disclosure outweighs the public interest of protecting confidentiality; or

iv)Approval under section 251 of the NHS Act 2006 is in place (most commonly for secondary uses this means the Health Research Authority's (HRA) Confidentiality Advisory Group (CAG) has given support under Regulation 5 of the Control of Patient Information Regulation 2002 (COPI) for a specific project).

Having UK GDPR legal bases for personal data processing does not remove the need to seek permission or an appropriate legal basis (e.g. Section 251 support) for using the data for secondary purposes. This links into the Data Protection Act principle of purpose limitation which means that you can only process data for the specified, explicit, and legitimate purposes and not further process it in a manner that is incompatible with those original purposes.

Legal Gateways.xlsx

Relevant Guidance

Partners will rely on the following guidance to adhere to principles defined in this agreement.

National Guidance:

- Working together to safeguard children (Department for Education)
- Information sharing advice for safeguarding practitioners (Department for Education)
- 10 step guide to sharing information to safeguard children (Information Commissioner's Office)
- MAPPA Guidance (Ministry of Justice, National Offender Management Service, HM Prison Service)
- The Caldicott Principles (National Data Guardian)
- Serious Violence Duty (Home Office)
- Code of Practice: Police and Information Records Management and associated guidance issued by the College of Policing

- Childrens Act 1989 and 2004
- Common Law Duty and Confidentiality
- Crime and Disorder Act 1998
- UK General Data Protection Regulation 2016
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Education Act 2002
- The Health and Social Care(Safety and Quality) Act 2015
- Human Rights Act 1998
- Local Government Act 1972 and 2000
- National Health Services Act 2006
- Care Act 2014
- Care & Support Statutory Guidance
- Mental Capacity Act 2005
- Information Commissioner
    - Data Sharing Code of Practice
    - Explaining decisions made with AI

Local Guidance:

- Pan Lancashire Joint Working and Information Sharing Protocol August 2023
- Education Management System (EMS) and Schools' Data Feed Data Sharing Agreement for Partners Between LCC and Partners (All state-funded schools within Lancashire Local Authority)Local organisational Standard Operational Procedures (SOP) for sharing with external agencies

Appendix 4 – Joint Resources

Name of Document/Tool	Description	Source Organisation(s)
e.g. Training material, fair processing notices, DSA & DPIA templates, policies, guidance etc.	*e.g. Lawful Basis and Legal Framework document agreed by all statutory partners and shared with all non-statutory partners.*	*e.g. the content has been produced by the Police, Health Trust and the Local Authority, input from Bernardo's has been received and included.*

Appendix 5 – Partners to this agreement

Organisation	Address	ICO registration number	General contact person	General contact details	IG contact person	IG contact details	ODS number
Lancashire County Council	PO BOX 78, COUNTY HALL, PRESTON, ENGLAND, PR1 8XJ	Z542705X	Medina Patel	Medina.Patel@lancashire.gov.uk	Joanne Winston	dpo@lancashire.gov.uk	323
Blackpool Borough Council	Town Hall Blackpool FY1 1NA	Z5720508	Sarah Hargreaves or Sarah Rahmat	Sarah.Hargreaves@blackpool.gov.uk or Sarah.Rahmat@blackpool.gov.uk	Jonathan Pickup	dataprotectionofficer@blackpool.gov.uk	325
Blackburn with Darwen Borough Council	Town Hall King William Street Blackburn Lancs BB1 7D	Z6166514	Abdul Aziz-Ghiwala	abdulaziz.ghiwala@blackburn.gov.uk	Sarah Critchley	sarah.critchley@blackburn.gov.uk	324
NHS Lancashire & South Cumbria Integrated Care Board	Fishergate Hill Level 3 Christchurch Precinct County Hall Preston Lancashire PR1 8XB	ZB392902	SPOC	Lscicb.safeguarding@nhs.net	Hayley Gidman	mlcsu.dpo@nhs.net	QE1
Lancashire Constabulary	Headquarters Saunders Lane Hutton	Z4886309	Vulnerability Governance Unit (VGU)		Carl Melling	InformationSharingAgreements@lancashire.police.uk	

Organisation	Address	ICO registration number	General contact person	General contact details	IG contact person	IG contact details	ODS number
	Preston PR4 5SA		Lancashire Constabulary HQ				
Blackpool Teaching Hospital NHS Foundation Trust	Whinney Heys Road, Blackpool, FY3 8NR	Z5052220	Suzanne Smith	suzanne.smith79@nhs.net	Samuel Winter	samuel.winter@nhs.net	RXL
East Lancashire Hospital Trust							
Lancashire Teaching Hospitals NHS Foundation Trust	Royal Preston Hospital Sharoe Green Lane Fulwood, Preston PR2 9HT	Z6929649			Louise Magee	dpo@lthtr.nhs.uk	RXN
Lancashire and South Cumbria NHS Foundation Trust	LSCFT HQ Sceptre Point Sceptre Way Bamber Bridge Preston PR5 6AW	Z6710592	IG.Queries@lscft.nhs.uk	IG Queries Mailbox	Michelle Brammah	dpo@lscft.nhs.uk	RW5
Southport and Ormskirk Hospital Trust							
HCRG Care Group							
University Hospitals of							

Organisation	Address	ICO registration number	General contact person	General contact details	IG contact person	IG contact details	ODS number
Morecambe Bay Trust							
National Probation Service North West	Preston Probation Office Diadem House 2 The Pavilions Port Way Preston PR2 2YB	Z5679958	Elaine Seed	Elaine.Seed@justice.gov.uk	Kevin Kelly	Kevin.kelly@justice.gov.uk	N/A
Lancashire Fire and Rescue Service	Garstang Road, Fulwood, Preston PR2 3LH	Z8579219	Caroline Robinson	carolinerobinson@lancsfirerescue.org.uk	Robert Shaw	robertshaw@lancsfirerescue.org.uk	
North West Ambulance Service	Ladybridge Hall Bolton BL1 5DD	Z9603234	Jane Whittaker	Jane.Whittaker@nwas.nhs.uk	Joanne Moran	Joanne.Moran@nwas.nhs.uk	RX7