Overarching Tier 1 Children Safeguarding Information Sharing Agreement (ISA)

For Durham Safeguarding Children Partnership (DSCP)

1 Introduction

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

It has been frequently recognised in local and national reviews of practice that failing to share information at critical times has costs lives or led to detrimental outcomes. A fear of sharing sensitive information must not be a blocker to safeguarding and promoting the welfare of children at risk. The relevant UK government departments and independent non-departmental government bodies responsible for protecting children and/or regulating data protection therefore set out policy, legislation, and statutory guidance on how the protection system should work and data protection compliance is achieved at the same time. Those pieces of legislation are in place for the relevant sharing partners to be used to justify information sharing and to allow it in a safe and legal way. Some legislation puts a duty on organisations to share and others provide with the power to do so.

The partners of this agreement are aware and understand their legal responsibilities to deliver safeguarding to children and their families as defined (amongst others) in the:

Children Act 2004, Section 10
Each local authority must make arrangements to promote co-operation between partners (including the ICB, Police, Schools and other) 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).

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 children experiencing and at risk of abuse and harm and for wider public protection. For this reason, this Tier 1 DSA applies to all areas of children's 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, see appendix 1 for further details.

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.

2 Contents

3 Administration

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

Organisation(s)
County Durham and Darlington Fire and Rescue Service
County Durham and Darlington NHS Foundation Trust (CDDFT)
County Durham and Darlington Probation Delivery Area, North East Probation Region as part of the HM Prison and Probation Service
Domestic Abuse Service; Harbour
Drug and Alcohol Service; HumanKind
Durham Community Action
Durham Constabulary
Durham County Council
Harrogate and District NHS Foundation Trust (HDDFT)
North East Ambulance Service NHS Foundation Trust
North East and North Cumbria Integrated Care Board (ICB)
Tees, Esk and Wear Valleys NHS Foundation Trust (TEWV)
Other strategic partners that have responsibilities to address issues relevant to safeguarding children

General:

Date Tier 1 DSA comes into force:	February 2024
Last review:	April 2024
Date for review of DSA:	April 2025 or as required (annual schedule)
DSA Owner (Organisation):	Durham County Council
DSA Author(s):	Vicki Vickerson (DCC), Antje Carpenter (NHS SCW CSU)

Version control:

Version	Date	Author	Edit/Update
V0.1 Draft	05/12/2023	Antje Carpenter, SCW	First draft for consideration
V0.2 Draft	15/01/2024	Antje Carpenter, SCW	Draft update including partner comments
V0.3 Draft	16/01/2024	Vicki Vickerson, DSCP	Draft update
V0.4 Draft	17/01/2024	Antje Carpenter, SCW	Inclusion of qualifying standard and other relevant content as per Task and Finish Group discussion.
V0.5 Draft	01/02/2024	Antje Carpenter, SCW	Inclusion of partner feedback received
V0.6 Draft	06/02/2024	Antje Carpenter, SCW	Inclusion of further partner feedback received
V0.7 Draft	28/02/2024	Vicki Vickerson, DSCP	Administration and agencies updated
V0.8 Final	29/04/2024	Vicki Vickerson, DSCP	Administration, Section 18 and Appendix 5 updated to reflect signatories

4 Scope

This Tier 1 Information Sharing Agreement applies to organisations operating within Durham. It is a multi-agency agreement between Local Authorities, Integrated Care Board (ICB), NHS Organsiations, Police, Education, Probation and Voluntary Sector Organisations. A full list of signatory organisations can be found under section 3 Administration and in Appendix 5. The Agreement covers the sharing of personal and special category data about children and their families for safeguarding reasons. This agreement is not contractually binding but is setting good practice standards that the sharing partners are required to meet.

The Durham Safeguarding Children Partnership (DSCP) is established in accordance with the Children Act 2004 (as amended by Children and Social Work Act 2017) and Chapter 3 Working Together to Safeguard Children 2023. The DSCP provides the safeguarding arrangements under which the safeguarding partners and relevant agencies work together to coordinate their safeguarding services, identify, and respond to the needs of children in County Durham, commission and publish local child safeguarding practice reviews and provide scrutiny to ensure the effectiveness of the arrangements.

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

a) Durham County Council
b) North East and North Cumbria Integrated Care Board (ICB)
c) Durham Constabulary

The three statutory 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 safeguarding incidents.

The statutory partners are supported by wider partner agencies as follows:

- Chairs of the DSCP Sub-Groups
- County Durham and Darlington NHS Foundation Trust (CDDFT)
- Designated Doctor for Safeguarding Children
- Domestic Abuse Services; Harbour
- Drug and Alcohol Services; HumanKind
- Durham County Council Children and Young People's Services
- Durham County Council Education and Skills

- DSCP Business Manager (for support)
- Harrogate District NHS Foundation Trust (HDDFT)
- Independent Scrutineer
- North East Ambulance Service (NEAS) NHS Foundation Trust
- North East and North Cumbria Integrated Care Board
- North East Probation Region
- Tees, Esk and Wear Valleys NHS Trust (TEWV)
- Voluntary and charitable organisations; Durham Community Action

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 information sharing agreement. This agreement should not be seen as an alternative to a Tier 1 agreement, Tier 2 agreements 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)).

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

a) **providing help and support to meet the needs of children as soon as problems emerge**
b) **protecting children from maltreatment, whether that is within or outside the home, including online**
c) **preventing impairment of children's mental and physical health or development**
d) **ensuring that children grow up in circumstances consistent with the provision of safe and effective care**
e) **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**
f) **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

a. preventing harm;
b. promoting the welfare of a child; and
c. 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 but also sharing for prevention and early intervention in less immediate or high-risk situations.

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 assistance in the form of counselling, advice, early help support, prevention and guidance as well as referring individuals to other organisations and charities within their network.

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 children who require safeguarding intervention and to facilitate the statutory functions of the Childrens Safeguarding Partnerships. 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 the organisations (multi-agency/integrated working) that are parties to this agreement with the intention of:

- Protecting children'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 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 their families.
- 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.
- Collaborating, sharing and co-owning the vision for how to achieve improved outcomes for vulnerable children.
- Challenging appropriately and holding one another to account effectively.
- Sharing information effectively to facilitate more accurate and timely decision making for children and families.
- Ensuring that shared learning is promoted and embedded in a way that local services for children and families 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

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 whole 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 young people at risk of harm across Durham 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 meet the legal requirements for Data Protection, 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 and safely.
Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of personal information from other organisations, employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that data is not disclosed illegally or inappropriately. 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 will need to be completed and shared with the relevant partners as appropriate. This agreement does not replace the need to conduct a Data Protection Impact Assessment of the information or processes involved.
An individual's personal information must be complete and up to date and will only be disclosed where there is a legal purpose/justification 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 proportionate, 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 of this kind will only be taken on statutory grounds and must be linked to a detrimental effect on the physical or mental wellbeing 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. Data concerning deceased individuals is not covered by the UK GDPR or DPA18 but the Access to Health Creds Act 1990.
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 Data Protection Act (2018).
All organisations agree that appropriate training will be given to staff so that they are aware of their responsibilities to ensure personal and special category information is processed lawfully (including the annual completion of data protection and information security training by all relevant staff).
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 and incidents relating to the processing/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. Full and robust justification is required and must be documented.
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 and if they do not do so, the safeguarding partners may take legal action against them.

The qualifying standard for organisations to achieve to sign up to this sharing agreement is achievement of 'standards met' to the current version of the Data Security & Protection Toolkit (Data Security and Protection Toolkit (dsptoolkit.nhs.uk)) or equivalent depending on the type of organisation.

If 'standards met' has not been achieved (organisation failed, not required to complete the DSPT, DSPT expired) organisations will be asked to confirm their plans (including the completion of the DSPT voluntarily) and share the relevant details. The statutory partners will consider the position of the organisation and make recommendations regarding the signing of the agreement.

The Fire and Rescue Service must adhere to the Approved Fire Standard. The Police must adhere to the Authorised Professional Practice (APP) for Police Information.

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 Information 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 safeguarding sharing can be found in **Appendix 3**.

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

a. UK General Data Protection Regulation (GDPR)
b. Data Protection Act (DPA) 2018
c. Human Rights Act 1998 (article 8)
d. 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 Information Sharing Agreement. 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)(b) – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the filed of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

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.

Article 10 Criminal offence data processing meeting a specific condition in Schedule 1 Data Protection Act 2018.

The Police's underlying power to share personal data is derived from (i) Common Law Policing Purposes which may be summarised as: protecting life and property, preserving order, preventing the commission of offences, and bringing offenders to justice and/or (ii) any duty or responsibility arising from statute or other rule of law including court order and royal prerogative.

The signatories of this agreement understand that 'Consent is one lawful basis, 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 DPO for review.

8 Guidance

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

National Guidance:

- Working together to safeguard children 2023 (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)
- Management of Police Information (MoPI) statutory Code of Practice College of Policing

Local (or locally used) Guidance:

- When a Child Dies – a guide for families and carers (lullaby-cdr-booklet.pdf (lullabytrust.org.uk))
- Child Death Review Statutory and Operational Guidance (England) (publishing.service.gov.uk)
- Information Sharing (proceduresonline.com)
- Agreement to Request Early Help by Someone with Parental Responsibility; early help assessment2 (proceduresonline.com)
- Child Exploitation Intelligence and Information Submission Form; NEW Partnership Information Sharing form.pdf (proceduresonline.com)
- Operating Procedures for Children and Young People who are Missing from Home or Care; Local Resources (proceduresonline.com)
- Child Safeguarding Practice Reviews (proceduresonline.com)
- Community Safety Information Sharing Protocol (countydurhampartnership.co.uk)

9 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.

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

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)
- A position/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
- Multi factor authentication

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.

10 Proportionality and necessity

The data relevant under this Tier 1 Information 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 and proportionate to the purposes should be shared with those partners who have justified that they 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 Information 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 and apply anonymisation or pseudonymisation if and as possible.

11 Retention

Records will be retained and disposed of in accordance with data protection legislation requirements and national and local/organisational data retention 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 (including considerations around copies of data). 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 Information 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 Records Management Code of Practice to inform decision making (not applicable to children social care). Durham Constabulary (and other Police Forces) must consider and also comply with the statutory College of Policing Management of Police Information (MoPI) Code of Practice and 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 partners' 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 Information 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 Information 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 consultative 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 DSCP should be forwarded to Durham County Council's Data Protection Officer dpo@durham.gov.uk to coordinate the appropriate response. When a partner agency requires cooperation from the DSCP or SAB to respond to a Subject Access Request they should contact the relevant Business Support Team Manager to ensure appropriate liaison with the Durham County Council's Data Protection Officer.

13 Transparency

Each organisation must be clear, open and transparent with data subjects (including parents/carers) 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 agree an approach 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). 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).

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' or equivalent on a routine basis).

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 information 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. Reportable incidents (data breaches) must be notified to the ICO within 72h of identifying the breach. As such, sharing partners must inform the responsible controller (DPO) as soon as possible (where they become aware of an incident that they are not responsible for or are only partially responsible for). 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.

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).

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. Lessons learnt from investigations will be shared with partners through the Board where appropriate.

Complaint handling should follow a similar path; however, they are unlikely to require such priority/urgency unless they are intrinsically linked to an incident.

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.

Child Death Reviews
The process of systematically reviewing the deaths of children is grounded in respect for the rights of children and their families, with the intention of learning what happened and why, and preventing future child deaths. The purpose of a review and/or analysis is to identify any matters relating to the death, or deaths, that are relevant to the welfare of children in the area or to public health and safety, and to consider whether action should be taken in relation to any matters identified. If child death review partners find action should be taken by a person or organisation, they must inform them. Child Death review partners may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process - the person or organisation must comply with the request, and if they do not, the child death review partners may take legal action to seek enforcement. All local organisations or individual practitioners that have had involvement in the case should co-operate, as appropriate, in the child death review process carried out by child death review partners. All local organisations or individual practitioners should also have regard to any guidance on child death reviews issued by the government. The Child Death Overview Panel may receive requests for access to records from family members and each request will be considered and responded to on a case by case basis. In the immediate aftermath of a child's death, a copy of *When a Child Dies – a guide for families and* carers (details see under section 8. Guidance) should be offered to all bereaved families or carers in order to support them through the child death review process. For further information see Chapter 6 of Working Together to Safeguard Children 2023.

Child Death Overview Panel (CDOP)

This describes some of the statutory requirements placed upon child death review (CDR) partners, and the functions that they are expected to carry out. It outlines the function of an independent and multi-agency panel that should be established to scrutinise all aspects of a child's death, using evidence generated in the steps which precede this stage of the overall child death review process. This is known as a Child Death Overview Panel (CDOP) or equivalent.

CDR partners are free to establish the specific structure to conduct this independent multi-agency scrutiny based on local need, using the information provided throughout the preceding steps of the review process. However, they should ensure that whatever structure they use should as far as possible ensure standardised output to enable thematic learning at national level. In all cases throughout this guidance, the body conducting the CDR partners review is identified as a CDOP. In making arrangements to review child deaths, CDR partners should establish a structure and process to review all deaths of children normally resident in their area and, if appropriate and agreed between CDR partners, the deaths of children not normally resident in their area but who have died there.

Multi Agency Safeguarding Hub (MASH)

The Multi Agency Safeguarding Hub (MASH) screen, gather, analyse, and share information relating to referrals about children in County Durham who may be at risk of harm, or who need support services. This makes sure that all the key information about a child and their family is shared at this critical time.

The MASH links with other key agencies who will be asked to provide information where necessary.

The MASH will screen and share information relating to referrals that are made about children where there are concerns for their welfare or their safety. The MASH is designed to ensure that all the available information from key agencies about a child and their family is shared in a timely way at this critical decision-making point. All agencies have access to their own IT systems within the MASH and so can quickly and easily share information that they hold about children and their families. Any new multi-agency information will then be stored centrally on the social services information database and be added to the original referral information.

Tier 2 ISA has been reviewed (Dec 2023) and an additional review is currently underway (Feb 2024).

Multi Agency Risk Assessment Conference (MARAC)

A Multi Agency Risk Assessment Conference (MARAC) is a meeting where information is shared on the highest risk Domestic Violence and Abuse cases between representatives of the local police, probation, health, children and adults Safeguarding bodies, housing practitioners, substance misuse services, independent domestic abuse advisers (IDAAs) and other specialists from the statutory and voluntary sectors.

The four aims of a MARAC are as follows:

- To safeguard adult victims who are at high risk of future domestic violence;
- To make links with other public protection arrangements in relation to children, people causing harm and adults with care and support needs;
- To safeguard agency staff; and
- To work towards addressing and managing the behaviour of the person causing harm.

It puts in place various plans and actions in relation to the safety and well-being of the identified person, and if appropriate, their children. The MARAC process does not override pre-existing procedures within organisations where issues of Child Protection are concerned.

Multi Agency Public Protection Arrangements (MAPPA)

Multi-Agency Public Protection Arrangements (MAPPA) are the set of arrangements through which the Police, Probation and Prison Services work together with other agencies to manage the risks posed by violent and sexual offenders living in the community in order to protect the public.

The process where the Lead Agency decides what Level an offender should be managed at is referred to a ‘thresholding’; the process considers the various requirements for management at each level as well as offender risk and need.

MAPPA is not a statutory body but is a mechanism through which agencies can co-ordinate their approach to meeting statutory responsibilities and protect the public. Agencies always retain their full statutory responsibilities and obligations and all information that is shared under MAPPA remains the responsibility of the agency that owns it.

Child Safeguarding Practice Reviews

The purpose of reviews of serious child safeguarding cases, at both local and national level, is to identify improvements to be made to safeguard and promote the welfare of children. Learning is relevant locally, but it has a wider importance for all practitioners working with children and families and for the government and policy- makers. Understanding whether there are systemic issues, and whether and how policy and practice need to change, is critical to the system being dynamic and self-improving. Reviews should seek to prevent or reduce the risk of recurrence of similar incidents.

Locally, safeguarding partners must make arrangements to identify and review child safeguarding cases which in their view, raise issues of importance in relation to their area. They must commission and oversee the review of those cases where they consider it appropriate for a review to be undertaken.

Serious child safeguarding cases are those in which:

- abuse or neglect of a child is known or suspected **and**
- the child has died or been seriously harmed

The safeguarding partners must supervise the review to ensure that the reviewer is making satisfactory progress and that the review is of satisfactory quality. The safeguarding partners may request information from the reviewer during the review to enable them to assess progress and quality; any such requests must be made in writing.

Reviews are about promoting and sharing information about improvements, both within the area and potentially beyond, so safeguarding partners must publish the report, unless they consider it inappropriate to do so. In such a circumstance, they must publish any information about the improvements that should be made following the review that they consider it appropriate to publish.

When compiling and preparing to publish the report, the safeguarding partners should consider carefully how best to manage the impact of the publication on children, family members, practitioners and others closely affected by the case.

The safeguarding partners should ensure that reports are written in such a way so that what is published avoids harming the welfare of any children or vulnerable adults involved in the case.

Channel and Prevent

The Prevent Strategy aims to stop people being drawn into terrorist and extremism related activity. Referral processes are in place for personalised information to be shared with Durham Constabulary for assessment. Where the police assess the individual as requiring a referral to the Channel Programme, Durham County Council has a statutory duty to ensure that a Panel is in place to assess the extent to which identified individuals are vulnerable to being drawn into terrorism and developing an appropriate support plan.

The Channel Panel is dependent on the co-operation and coordinated activity of partners to ensure that those vulnerable to radicalisation receive support before they are exploited by those that would want them to embrace terrorism or engage in criminal terrorist related activity.

Consent is required from the individual (and/or parent) to engage and receive a support package with the Channel Panel. A confidentiality declaration is agreed to by all participating agencies attending the Channel Panel.

The multi-agency involvement in the Channel process is essential to ensure that vulnerable individuals have access to a wide range of support, from access to specific services provided by local authorities to diversionary activities.

Information sharing is an essential part of the process to determine whether an individual requires support, and if so, what that should consist of.

Operation Encompass

Data on Domestic Abuse is shared between partners to build a picture of the prevalence and nature of domestic abuse in County Durham in respect of victims and perpetrators. Operation Encompass provides a process for notifying a designated Key Adult within schools when a student was present in a household at the time when an incident of domestic abuse was recorded as having taken place. The school can then provide immediate appropriate level support to the child who may have been a victim or witness to the abuse, whilst in attendance at school.

Harm outside the home

Criminal and sexual exploitation is co-ordinated under the Child Exploitation Team to manage those young people at significant risk. This team is comprised of Police and Children's Social Care staff with the aim of reducing this risk via education, support and intervention.

County Durham has a dedicated multi-agency ERASE Team developed to improve our response to criminal and sexual exploitation (CSE). The ERASE Team aim to intervene early with young people at risk of CSE or who go missing from care or their own homes and ensure a proportionate response. All CSE intelligence will be shared with operational meetings to plan responses and disruption to offenders.

Young people are referred into the Child Exploitation Team by professionals following the completion of a Child Exploitation Matrix.

The Child Exploitation Matrix is a document which allows professionals to assess the level of risk of criminal or sexual exploitation of a child. The matrix is designed allow a risk grading of young people at risk of both criminal and sexual exploitation.

Section 47 (Children Act 1989)

When children's social care receives a referral and information has been gathered during an assessment (which may have been very brief), in the course of which a concern arises that a child maybe suffering, or likely to suffer, significant harm, the local authority is required by Section 47 of the Children Act 1989 to make enquiries. The purpose of this multi-agency enquiry and assessment is to enable the agencies to decide whether any action should be taken to safeguard and promote the wellbeing of the child. Any decision to initiate an enquiry under Section 47 must be taken following a Strategy Meeting/Discussion.

The social worker together with their manager must decide at what point and whether to seek parental permission to undertake multi-agency checks. If the manager decides not to seek permission, they must record the reasons why, for example it may:

- Be prejudicial to the child's safety and wellbeing;
- Have serious concern about the behaviours of the adult;
- Have serious concern that the child would be exposed to immediate risk of harm.

Where permission is sought from parents and carers and denied, the manager must determine whether to proceed, and record the reasons for the decision they make.

Each agency has a duty to assist and provide information in support of child protection enquiries. The social worker must contact the other agencies involved with the child to inform them that a child protection enquiry has been initiated and to seek their views. The relevant agency should be informed of the reason for the enquiry, whether or not parental consent (to participate) has been obtained and asked for their assessment of the child in the light of information presented.

The social worker must contact the other agencies involved with the child who have not been involved in the Strategy Discussion to inform them that a Section 47 Enquiry has been initiated and to seek their views. The checks should be undertaken directly with involved professionals wherever possible.

The relevant agency should be informed of the reason for the enquiry, as well as whether or not parental consent (to participate) has been obtained, and asked for their assessment of the child in the light of information presented.

Agency checks should include accessing any relevant information that may be held in other parts of the United Kingdom or in any other country.

Section 17 (Children Act 1989)

Under Section 17(1) of the Children Act 1989, local authorities have a general duty to safeguard and promote the welfare of children within their area who are in need.

Assessments are undertaken of the needs of individual children to determine what services to provide, and action to take. They may be carried out:

- To gather important information about a child and family;
- To analyse their needs and/or the nature and level of any risk and harm being suffered by the child. Also see: Risk Assessments;
- To decide whether the child is a Child in Need (Section 17) and/or is suffering or likely to suffer Significant Harm (Section 47); and
- To provide support to address those needs to improve the child's outcomes to make them safe.

Child Protection Notifications

The DSCP Partnership has responsibilities under the DSCP Child Protection Procedures for the following notifications:

a) National Missing Person Alerts
b) At Risk to Children Notifications
c) Durham Child Protection Conference Activity
d) Children on a Child Protection Plan in another Local Authority residing in County Durham

Any disclosure or sharing of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidence, and the data protection legislation.

Disclosures of information will be:

a) on a case by case basis
b) in an agreed format where this is provided
c) in accordance with any data workflow agreements
d) proportionate
e) with a minimum amount of information necessary to achieve the purpose
f) only with those individuals who have a right to access the information

Safeguarding partners should co-operate as appropriate and be aware of their own responsibilities under the relevant information law and have regard to guidance provided by the Information Commissioner's Office when receiving such information.

It should be noted that the above list is not exhaustive but any data sharing for Safeguarding Children purposes will still fall under this agreement.

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 protocol will be shared with all signatories, processors and relevant parties for the purpose of upholding the principles of this agreement.

It is intended that this overarching Tier 1 Information Sharing Agreement contains high level principles and partner commitments only. It will therefore be reviewed annually to establish if the sharing remains necessary, still operates as intended and, has or is, achieving the intended benefits, unless legislative changes, organisational boundaries, best practice or other significant changes require immediate action. The monitoring and review of this protocol will be undertaken by Durham County Council.

Subject to there being no significant changes, the agreement may be extended by a further two years 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.

18 Signatories

If this Information Sharing Agreement is published to a system that manages signatures/agreement, then this section can be removed.

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: County Durham and Darlington Fire and Rescue Service
Name: Keith Carruthers
Role: Deputy Chief Fire Officer
Email: keith.carruthers@ddfire.gov.uk
Signature:
Date signed: 29 May 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Jon Bell, Information Services Manager

2. Signed on behalf of: County Durham and Darlington NHS Foundation Trust
Name: Emma McBeth
Role: Interim Deputy Associate Director for Safeguarding, Patient Experience & Chaplains
Email: emma.mcbeth@nhs.net
Signature:
Date signed:
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Lisa Natrass, Head of Data Security & Protection Data Protection Officer

3. Signed on behalf of: County Durham and Darlington Probation Delivery Area, North East Probation Region as part of the HM Prison and Probation Service
Name: Karen Blackburn
Role: Head of Area
Email: karen.blackburn@justice.gov.uk
Signature:
Date signed: 24 May 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Saphron North (Probation Officer) or Karen Bruce (Regional Information Security and Assurance Lead)

4. Signed on behalf of: Domestic Abuse; Harbour
Name: Lesley Gibson
Role: Chief Executive
Email: lesleygibson@myharbour.org.uk
Signature:
Date signed: 20 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Rachael Williamson (Service Manager)

5. Signed on behalf of: Drug and Alcohol Service; Humankind
Name: Victoria Haughey
Role: Area Manager
Email: victoria.haughey@humankindcharity.org.uk
Signature:
Date signed: 20 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Jane Curtis (Safeguarding Team)

6. Signed on behalf of: Durham Community Action
Name: Kate Burrows
Role: Executive Director
Email: kate.burrows@durhamcommunityaction.org.uk
Signature:
Date signed: 04 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Abby Thompson (Volunteering Manager)

7. Signed on behalf of: Durham Constabulary
Name: Nicola Lawrence
Role: Temporary Detective Chief Superintendent, Crime Command, (Safeguarding, Complex and Serious Investigations, Forensics and Intelligence)
Email: nicola.lawrence@durham.police.uk
Signature:
Date signed: 24 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Leigh Davison (Head of Information Rights and Disclosure Unit)

8. Signed on behalf of: Durham County Council
Name: Keith Forster
Role: Service Manager, Operational Support (Caldicott Guardian)
Email: Keith.forster@durham.gov.uk
Signature:
Date signed: 09 July 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Data Protection Officer (DPO@durham.gov.uk)

9. Signed on behalf of: Harrogate and District NHS Foundation Trust (HDDFT)
Name: Sam Layfield
Role: Data Protection Officer
Email: hdft.dataprotectionofficer@nhs.net
Signature:
Date signed: 13 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Jo Higgins (Information Governance Manager)

10. Signed on behalf of: North East Ambulance Service (NEAS)
Name: Kathrine Noble
Role: Medical Director and Caldicott Guardian
Email: Katherine.Noble@neas.nhs.uk
Signature:
Date signed: 20 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Seema Srihari, Information Governance Manager and Trust Data Protection Officer

11. Signed on behalf of: North East and Cumbria Integrated Care Board (ICB)
Name: Neil O'Brien
Role: Executive Medical Director
Email: neilobrien@nhs.net
Signature:
Date signed: 24 May 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Liane Cotterill (Senior Governance Manager & Data Protection Officer)

12. Signed on behalf of: Tees Esk and Wear Valleys NHS Foundation Trust (TEWV)
Name: Beverley Murphy
Role: Chief Nurse
Email: beverley.murphy7@nhs.net
Signature:
Date signed: 19 June 2024
Person/Post which is responsible on a day-to-day basis for monitoring compliance with this DSA: Nicki Smith, Associate Director for Nursing (Safeguarding)

Appendix 1 - Glossary of terms

Term	Definition
Ad-hoc data sharing	Justified 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)

Term	Definition
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.
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 and special category 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) as best practice to 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.

Term	Definition
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.
Information Commissioner's Office (ICO)	The UK's independent body set up to uphold information rights.
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 an 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.

Term	Definition
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.
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

By sharing information, we work better together, and this Tier 1 Information 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.

Routine Information sharing checklist (e.g. monthly, routine data sharing of specific indicators)

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. 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.

Ad-hoc Information sharing checklist (e.g. sharing ad-hoc during corridor conversation)

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 what information is necessary and relevant.

Is it fair to share in this way?
Consider less intrusive ways of fulfilling your purpose or reach your objectives and consider what individuals are expecting to happen to their data.

What are the benefits and what are the risks
Balance the benefits for an individual and/or the public against the risks of harm it could cause.

Where does the information originate from, does the source organisation need to be consulted?
Consider who is best placed to assess disclosure decisions around the risk of causing harm (e.g. interference with a police investigation, disclosure of details not knows to the recipient (adopted child).

What needs to be done to transfer the information securely
What technical and organisational measures are appropriate to ensure the security of the data.

Am I being transparent about information sharing
Consider what you have to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.

Check your organisational policies and procedures
What policies and processes around sharing are in place and what guidance must be considered.

Ask for help to make disclosure decisions
Consult colleagues, managers and Caldicott Guardians if you are unsure about sharing information.

Document your decision
Document your decision as appropriate.

Appendix 3 - Applicable Legislation

Appendix 3 Aplicable Legislation Durham.xl

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.*
Information Sharing and Consent - for People Working with Children	Importance of information sharing, how it can help prevent harm, legislation, consent, informed judgements and key questions.	DSCP, Me Learning available to all DSCP agencies
Partnership Information Sharing Form	This form should be used by partner agencies to share information with the police which has been gathered during the course of their work and may be of interest to law enforcement	Durham Constabulary via DSCP website
Child Exploitation Risk Assessment Information Form	This referral should be used where there is evidence or intelligence to suggest that a child is being or has been 'exploited'.	ERASE Exploitation Team via DSCP website

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
County Durham and Darlington Fire and Rescue Service	Belmont Business Park Durham, DH1 1TW	Z4757495	Keith Carruthers, Deputy Chief Fire Officer	keith.carruthers@ddfire.gov.uk	Jon Bell, Information Services Manager	jon.bell@ddfire.gov.uk	
County Durham and Darlington NHS FT	Appleton House, Lanchester Road, Durham DH1 5RD	Z1059396	Emma McBeth, Interim Deputy Associate Director for Safeguarding, Patient Experience & Chaplains	emma.mcbeth@nhs.net	Lisa Natrass Head of Data Security & Protection Data Protection Officer	l.nattrass@nhs.net	RXP
County Durham and Darlington Probation Delivery Area, North East Probation Region as part of the HM Prison and Probation Service	Corporation House, 9 Corporation Road, Darlington, Durham DL3 6TH	Z5679958	Karen Blackburn, Head of Area	karen.blackburn@justice.gov.uk	Karen Bruce, Regional Information Security and Assurance Lead)	NEPS.infosecurityassurance@justice.gov.uk	
Domestic Abuse Service; Harbour	8 Sydenham Road, Hartlepool TS25 1QB		Lesley Gibson, Chief Executive	lesleygibson@myharbour.org.uk	Rachael Williams, Service Manager	rachaelwilliamson@myharbour.org.uk	
Drug and Alcohol Service; Humankind	Inspiration House Unit 22 Bowburn North Industrial Estate Bowburn DH6 5PF	Z6654621	Vicky Haughey, Area Manager	victoria.haughey@humankindcharity.org.uk	Jane Curtis Safeguarding Team	jane.curtis@humankindcharity.org.uk	AJ6
Durham Community Action	9 St Stephen's Court, Low Willington, County Durham DL15 0BF	Z1931728	Kate Burrows, Executive Director	kate.burrows@durhamcommunityaction.org.uk	Abby Thompson, Volunteering Manager	Abby.Thompson@durhamcommunityaction.org.uk	
Durham Constabulary	Durham Constabulary HQ, Aykley Heads, Durham, Co. Durham, DH1 5TT	Z4895895	Nicola Lawrence, Temporary Detective Chief Superintendent Crime Command	nicola.lawrence@durham.police.uk	Leigh Davison (Head of IR & Disclosure/DPO)	leigh.davison@durham.police.uk or data.protection@durham.police.uk	

Durham County Council	Durham County Council County Hall Durham County Durham DH1 5UE	Z1808275	Keith Forster, Service Manager and Caldicott Guardian	Keith.forster@durham.gov.uk	DPO	DPO@durham.gov.uk	116
Harrogate and District NHS Foundation Trust	Harrogate District Hospital, Lancaster Park Road, Harrogate, North Yorkshire, HG2 7SX	Z7089698	Sam Layfied, Data Protection Officer	hdft.dataprotectionofficer@nhs.net	Jo Higgins, Information Governance Manager	jo.higgins@nhs.net	RCD
North East Ambulance Service	Bernicia House, Goldcrest Way, Newburn Riverside Business Park Newcastle Upon Tyne| NE15 8NY	Z4877768	Katherine Noble, Medical Director and Caldicott Guardian	Katherine.Noble@neas.nhs.uk	Seema Srinari, Information Governance Manager and Trust Date Protection Officer	Seema.Srihari@neas.nhs.uk	RX6
North East and North Cumbria Integrated Care Board (ICB)	Riverside House Goldcrest Way Newburn Riverside Business Park Newcastle upon Tyne NE15 8NY	ZB345018	Dr Neil O'Brien, Executive Medical Director	neilobrien@nhs.net	Liane Cotterill Senior Governance Manager & Data Protection Officer	liane.cotterill@nhs.net	00L
Tees, Esk and Wear Valleys NHS Foundation Trust	Nursing & Governance Directorate, Safeguarding Public Protection Team, Flatts Lane Centre, Normanby, TS6 0SZ	Z1387135	Beverley Murphy, Chief Nurse	beverley.murphy7@nhs.net	Nicki Smith, Associate Director for Nursing (Safeguarding)	nicki.smith3@nhs.net	RX3