Safeguarding Information Sharing Agreement (ISA)

Harm Outside the Home

between

the relevant statutory and non-statutory Durham Safeguarding Children Partnership (DSCP) partners and other relevant contributing community organisations within the Durham area

The creation of this Tier 2 Agreement is on the basis that all signatories accept and adopt the practices defined in the overarching Tier 1 Safeguarding Children Information Sharing Agreement hosted by the Durham Children Safeguarding Partnership (DCSP). Therefore, the baseline security and other specified requirements are not repeated because they are detailed in the Tier 1 ISA.

Content

1 Administration

The organisations (or types of organisation) below are signatories to this Information Sharing Agreement (see specified list of organisations and other relevant details in Appendix 1):

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

All partners to this agreement are controllers and are determining the purposes and means of processing.

General:

Date ISA comes into force:	October 2024
Last review:	September 2024
Data for review of ISA:	March 2025
ISA Owner (Organisation):	Durham Safeguarding Children Partnership (DSCP)
ISA Author:	Antje Carpenter, SCW Vicki Vickerson (DCC)

Version control:

Version	Date	Author	Edit/Update
V0.1 Draft	01/03/2024	Antje Carpenter	First draft for consideration
V0.2 Draft	30/04/2024	Antje Carpenter	Update to incorporate partner feedback
V0.3 Draft	08/05/2024	Vicki Vickerson	HOH professional update
V0.4 Draft	13/05/2024	Antje Carpenter	Group feedback update
V0.5 Draft	04/06/2024	Antje Carpenter	Update following Task and Finish Group
V0.6 Draft	01/07/2024	Vicki Vickerson	Update following Durham meeting
V0.7 Draft	09/07/2024	Antje Carpenter	Update following Task and Finish Group
V0.8 Draft	17/07/2024	Vicki Vickerson	Update following GD feedback
V0.9 Draft	15/08/2024	Vicki Vickerson	Update following T&F final review
V10.0 FINAL	13/09/2024	Vicki Vickerson	Update following Strategic CEG review

2 Purpose and benefits

Describe your sharing initiative/project (summary):

This Information Sharing Agreement aims to provide a framework in which partners can exercise their duty to share information to safeguard children and young people, specifically when considering information relating to harm outside the home.

It sets out clear expectations of Durham Safeguarding Children Partnership, Safe Durham Partnership, community safety and other partnerships to work to a shared understanding of the importance of timely, informed, respectful and purposeful gathering and sharing of information. It is recognised by all partners that sharing information as it emerges, can help minimise risks to children and young people and enable the provision of the right help and the right time.

Durham Safeguarding Children Partnership (DSCP) has highlighted harm outside of the home as a priority within the 2023 – 2026 business plan, this information sharing agreement has been agreed by all relevant partners to advance efficient and safe data sharing.

Harm outside the home can be defined as: Harm that can occur in a **range of contexts**, including school and other educational settings, peer groups, or within community/public spaces, and/or online. Children may experience this type of harm from other children and/or from adults. Forms of harm outside the home include exploitation by criminal and organised crime groups and individuals (such as county lines and financial exploitation), serious violence, modern slavery and trafficking, online harm, sexual exploitation, teenage relationship abuse, the influences of extremism which could lead to radicalisation and children missing and/or excluded from education. Children of all ages can experience harm outside the home.

Information necessary for safeguarding decisions in relation to children and young people is held by numerous statutory and non-statutory agencies. To deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information concerning a child and their circumstances to be available to them.

Further information relating to harm outside the home can be found via the DSCP website; Harm outside the home (durham-scp.org.uk)

Please also refer to the DSCP Child Exploitation HOH procedures for further details;

Contents (trixonline.co.uk)

- Child Exploitation (including Child Sexual Exploitation (2.0.5)
- Children from Abroad, including Victims of Modern Slavery (2.0.8)
- Children Missing from Home and Care (2.0.11)
- Gang Activity, Youth Violence and Criminal Exploitation Affecting Children (2.0.26)
- Online Safety: Children Exposed to Abuse through the Digital Media (2.02.22)
- Safeguarding Children and Young People Against Radicalisation and Violent Extremism (2.03.34) (2.03.34)
- Serious Violence Duty (4.0.3)

The procedures are aimed at all partners who come into contact with and therefore process information about children, young people and families, to ensure they are able to identify and address harm outside of the home.

Clearly set out your purpose(s) and benefits for sharing (include a description of the nature, scope and context):

The main **purposes** for managing information sharing through the harm outside the home (HOTH) approach are:

1. Utilising multi agency sharing and use of information to safeguard children and young people - to support early identification of, and response to, need.
2. Utilising information that is timely and purposeful - to ensure that information sharing practice prioritises a welfare response, and keeps families informed, while not undermining safety plans or live investigations
3. Information based risk assessment and decision making - identify through the best information available from inside and outside the home to the safeguarding partnership, those children and young people who require support or a necessary and proportionate intervention.
4. Victim identification and harm reduction - identify victims and future victims who are likely to experience harm from outside the home, and ensure partners work together to deliver harm reduction strategies and interventions.
5. Perpetrator identification – identify actual or potential perpetrators outside the home, to prosecute and/or support where appropriate.
6. Co-ordination of all safeguarding partners and wider partnerships, for example Safe Durham Partnership, to ensure that the needs of all vulnerable people are identified under full considerations of harms inside and outside of the child(ren) / young person's home and signposted to the relevant partner/s for the delivery and coordination of harm reduction strategies and interventions.
7. A process that acknowledges that the source of risk is from outside of the home, including online, therefore improving the likelihood of service user (child/young person/parent/family) engagement.

The main **benefits** for managing information sharing through the harm outside the home approach are:

1. Strengthens the requirements for partners and partnerships to share information as soon as problems emerge
2. Reasonable, relevant and proportionate information is shared with families, considering parents as partners, to enable them to safeguard children outside of their home.
3. Strengthens collaborative plans for children by reducing the risk of harm outside the home.
4. Enables professionals to be more responsive in identifying who is best placed to provide specific support for the child.
5. Harm outside the home plans are specific, measurable, achievable, realistic and timely (SMART), and are thoughtfully created by multiple agencies who are responsible for their delivery.
6. Removes barriers to effective information sharing
7. Coordinated and consistent response to all safeguarding concerns
8. Improves outcomes for children and young people at significant harm outside the home
9. Supports staff to use and share different forms of data appropriately and consider any unintended discrimination and / or harm that may arise through the gathering of intelligence or sharing of data and information.

3 Data Controller(s)

All partners to this agreement are contributing and viewing controllers and are determining the purposes and means of processing.

4 Data Sharing between partners

DPIA reference:	n/a
Personal identifiable data:	Examples of data that may be shared include: • Name of subject (child) and other family members, their carers and other persons whose presence and/or relationship with the subject child or children, is relevant to identifying and assessing the risks to that child (witnesses, perpetrators, peers etc.) • Age/date of birth of subject and other family members, carers, other persons detailed • School and educational information including school suspension data or data of children and young people on part-time timetables and those with persistent or severe absence • Housing and other partnership data relevant to the child and family which may affect the welfare of that child • Employment data
Special category data:	Examples of data that may be shared include: • Special category data relating to missing children • Ethnic origin of child, young person or family member • Relevant GP and health records, including sexual health • Sexual identity • Relevant data from Ambulance Service or Fire and Rescue Service • Education Health Care Plan (EHCP) and medical care plan, not in employment, education or training (NEET), Special Educational Needs and Disabilities (SEND) including Care Leavers and other vulnerabilities
Criminal offence data:	Examples of data that may be shared include: • Relevant Anti-Social Behaviour data • Sex offender data • Data relating to CSE & CCE • Criminal convictions • Youth Justice Service data

Health and social care professionals must have the confidence to share confidential information in the best interest of the individuals they look after as set out in this information sharing agreement. Principle 7 of the Caldicott Principles states that 'The duty to share information for individual care is as important as the duty to protect patient confidentiality'. The relevant professionals also must have the expertise to assure that data sharing around harm outside the home is limited to what is necessary, partners will not share more than needed for the purpose defined in this agreement. Partners who have ownership of the information should ensure that they are permitted to, and it is appropriate to share whilst adhering to Principle 7 as above.

When partners share information, they should record what has been shared, with whom and for what purpose. They should be clear on the nature of the information they are sharing, for example, Police may share non-conviction information (intelligence) as they believe that it poses a risk, therefore it can be shared.

Due to the complexity of the harm outside the home process, providing a prescriptive list of data fields to be shared is difficult. Any information that is shared in relation to harm outside the home will be decided on a case-by-case basis and must be relevant to the aims of this agreement. Not all the above information will be shared in every case; only relevant information will be shared on a case-by-case and 'need-to-know basis. Any restrictions on onward sharing must be communicated by the organisation the information originates from immediately and clearly (e.g. information which could interfere with a police investigation, information where the accuracy has not been verified etc.).

Harm outside the home information often originates from non-professionals (e.g. shop keepers, hotels, rented accommodation, caravan parks, public transport, taxis, fast food restaurants) who do not necessarily have the knowledge and expertise about the data protection principles as required. These non-professionals within the community often referred to as "places and spaces" are key in identifying harm outside the home and should be encouraged and supported to share information on a Public Task basis. All information received must highlight as a minimum where it originates from, if it is opinion or fact, if it has been verified. It is important that information that originates from 'places and spaces', such as those non professional's mentioned, and that we recognise that every interaction has the potential to be an intervention.

5 Lawfulness

Legal powers and gateways:
There are various Acts (refer to Tier 1 Safeguarding Children Information Sharing Agreement) and relevant Legislation which contain expressed or implied powers to share information. The act which is most relevant to this agreement and gives the statutory framework within which sharing around harm outside the home operates is the Children Act 2004 as amended by the Children and Social Work Act 2017.

Section 10 of the Children Act 2004 created a requirement for children's services to make suitable arrangements for co-operation between the relevant partners in order to improve the wellbeing of children in the authority's area. Statutory guidance for Section 10 of the Act states that good information sharing is key to successful collaborative working.

Each [local authority] in England must make arrangements to promote co-operation between
(a) the authority;
(b) each of the authority's relevant partners; and
(c) such other persons or bodies as the authority consider appropriate, being persons or bodies of any nature who exercise functions or are engaged in activities in relation to children in the authority's area.

The Act emphasises the importance of safeguarding the welfare of children by stating that relevant partner agencies (which include the Police, Children's' Services Authorities and CCG NHS Commissioning Boards (now ICB's) and other NHS statutory bodies) must ensure that functions are discharged having regard to the need to safeguard of children.

The Act emphasises that the authorities must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act as relating to a child's:

- physical and mental health and emotional well-being ('be healthy')
- protection from harm and neglect ('stay safe')
- education, training and recreation ('enjoy and achieve')
- the contribution made by them to society ('make a positive contribution')
- social and economic well-being ('achieve economic well-being')

An organisation needs to have a power to share data which may lie either in statute or in common law. The functions of a public sector organisation are set out in legislation, often referred to as 'legal powers and gateways'. Effective performance of those functions often requires the sharing of relevant personal and special category data. For some organisations the power to share data lies solely in common law although this is unlikely for public sector organisations. Knowing the legislation and common law duty or power that links to the relevant functions of safeguarding will provide a framework to enable the sharing of data to safeguard and protect children.

The Department for Education highlights in their 'The Working Together to Safeguard Children 2023' statutory guidance that 'practitioners will need to build an understanding of the context in which the harm is occurring and draw on relevant knowledge and information from the children and wider partners (it is highlighted within the guidance that this can include safeguarding partners and community partners such as those working in voluntary, private and statutory organisations who may come into contact with or be aware of the presence of children as they carry out their day-to-day roles in the community, for example, business owners, youth workers, faith and community leaders, park wardens etc.) in order to decide on the most appropriate interventions. Practitioners should consider the influence of groups or individuals perpetrating harm, including where this takes place online.'

For purposes other than law enforcement by competent authorities Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

Identify the UK GDPR Article 6 lawful basis and Article 9 condition(s):
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 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) – substantial public interest

Identify the appropriate condition(s) in UK law, set out in Schedule 1,2 & 3 of the DPA 18:
DPA 2018, Schedule 1, Part 2 – Substantial public interest conditions:
18) Safeguarding of children and individuals at risk

Please note that an Appropriate Police Document (APD) is required for the relevant conditions under Schedule 1, Part 2. Please check the DPA2018, Schedule 1 to establish the details.

The Police's underlying power to share personal data is derived from 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 any duty or responsibility arising from statute or other rule of law including court order and royal prerogative.

In terms of Data Protection legislation where the sharing is for one of the Law Enforcement Purposes – defined as the purposes of 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 – the sharing falls under the scope of Part 3 of the Data Protection Act 2018 (DPA) with the Police acting as a competent authority.

It is to note that the above content is relevant for the sharing of information concerning known and unknown children and young people (open or not open to services) but also adults or any other parties where their influence might affect issues relating to the wellbeing of, or, if relevant for the safeguarding of a child. Data protection legislation facilitates the sharing of data relevant in context of Harm Outside the Home if shared following the Data Protection principles. This might also include the sharing of information with third parties who can influence outcomes and input to define appropriate mitigations (e.g. sharing of details by police with public individuals, third party providers (e.g. youth club) in order to gain their assistance).

Non-interference – common law duty of confidentiality:
Non-interference with the common law duty of confidentiality describes the duty we have to keep personal information confidential under case law (not written out in a document (e.g., an Act) but based on previous court cases decided by judges). The law is applied by reference to those previous cases, so common law is also said to be based on precedent. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed unless it is lawful because 1) the individual has given consent, 2) where it is necessary to safeguard the individual, or others, or it is in the wider public interest, 3) where there is a legal duty to do so.

Please state here and explain how you will be satisfying Confidentiality:

1) Consent*:
2) Substantial Public Interest: **X**
3) Legal duty:

* Please note that consent under the common law is not the same as consent under data protection law. Consent under data protection law must be freely given, specific, and involve an affirmative action (UK GDPR Article 7 compliance). Consent under common law is satisfied if the individual(s) are aware and not objecting. This is 'implied' consent. Data Protection legislation requires individuals to be informed (see section 8) and allows them the opportunity to object (see section 9).

Non-interference – Human Rights Act 1998, Article 8:
Non-interference with Article 8 of the Human Rights Act 1998 guarantees the protection of individuals right to respect for private and family life, home and correspondence.

Please state here if and how you are able to interfere:

Yes:
(Partners might be able to interfere with the right if the action is lawful, necessary and proportionate in order to:

- protect national security
- protect public safety **X**
- protect the economy
- protect health or morals **X**
- prevent disorder or crime, or
- protect the rights and freedoms of other people)

No: n/a

6 How data sharing will be carried out

There are both structured and unstructured ways of receiving information that pertains to HOTH (linked to individuals), this may come in through established multi agency groups and processes like e.g. Child Exploitation Group, Front Door, MASH. Cases coming into the partnership might show HOTH relevance. The relevant partners hold information within their systems (including HOTH relevant information) and share this, as relevant, at the appropriate multi agency meetings. This might include information linked to known individual children but also information linked to individuals not known to any of the statutory services. It could also include broader areas (places and spaces) information. Sharing of all relevant information including HOTH, is essential in order for decision makers to be able to make fully informed choices around an individual's pathways.

Effective safeguarding relating to HOTH requires the support and involvement of the wider community and a range of partners. We must value the community experiences and build strong partnerships and collaboration with communities to ensure that they are part of a protection capacity against harm outside of the home.

It is important that harm outside of the home should not be viewed differently to any other form of welfare or safeguarding concern. Consent is one lawful basis to share information, but it is not required for sharing information in a safeguarding context, which includes **prevention** and **early intervention**, even in less immediate or high-risk situations. It is understood that sharing information on a public task basis and dispersing with consent where harm outside the home is a factor often poses challenges for practitioners when parents are not the persons causing the abuse, however this should never hinder or prevent safeguarding, we should aim to work with parents/carers whist ensuring that safeguarding is paramount which includes sharing relevant information. Further information is available via the Tier 1 Information Sharing Agreement, however, in summary, Working Together to Safeguarding Children 2023 highlights that "***fears about sharing information must not be allowed to stand in the way of safeguarding and promoting the welfare of children".***

While it is always good to work with the knowledge and understanding of those involved, including parents/carers, or even their agreement, it is important to remember that the lawful basis of consent is **not** required for sharing information in a safeguarding context, of which harm outside of the home, prevention and early intervention are included.

There is not currently a defined process for information which cannot directly be linked to an individual or a family that is not known to statutory services. Examples of information linked to broader areas rather than individuals could be groups of children or young people not currently open to the relevant services, spaces information, places information and other as relevant. Individual partners might have an established method for managing those records internally, but the partnership as a whole does not have a solution in place to date. It is an aspiration to establish working processes and procedures to store this type of information and manage it in a way so it can be linked to individuals and accessed by all relevant partners as required and therefore help achieve the benefits needed in order to safeguard the community as a whole. It is therefore appropriate for each organisation to make the best decision possible as to where the most appropriate place to retain this information is.

The appropriate mechanism/method by which data will be shared and held:
All partners to this agreement, who are sending or receiving sensitive personal data electronically, must have a secure e-mail established. If secure email is not available, for example, due to technical failure, then information will be shared in person.

All information will be recorded centrally in Liquid Logic by the Local Authority. However other agencies can and are encouraged to keep their own records if required so that each organisation is aware of which and how its information is being used. Other agencies or services may be passed information, where appropriate, when further interaction with a child is required. This information may be stored electronically within that agency or service recording systems.

All partners must adhere to confidentiality instructions for specific sharing methods as they are communicated (e.g. instructions on how to handle meeting minutes, instructions on how to handle copies of data (e.g. deletion of emails, paper copies etc.), instructions around disclosure risks (e.g. interference with an investigation, risk of harm to an individual etc.). Specific confidentiality expectations might be recorded within meeting minutes, Terms of Reference, Confidentiality statements verbal or other.

The likelihood of information being solely HOTH is small (with exception of information not related to an individual or open to any of the relevant services and places and spaces information). Partners therefore have to follow policy and procedure (including retention and destruction) linked to general information sharing (e.g. retention for service user records).

Specific (different) retention periods might be established for documents like meeting minutes and must be recorded within the terms of reference, confidentiality statements or other instructions to assure information is not kept longer then required. The handling of copies including personal information (including retention) should be defined before they are shared.

Information about children which are unknown to the relevant services and/or adults not linked to a child must be recorded in a secure and restricted area outside the appropriate system if the clinical system does not allow for information of this type to be stored. Access management must be defined and recorded, and retention periods must be established considering the business need and adhering to relevant statutory and non-statutory guidance (e.g. Records Management Code of Practice).

7 Processing outside of the UK (Compliance with Article 45 of the UK GDPR

Please state below if any personal data will be transferred outside the UK:
No personal data will be transferred outside of the UK.

If in exceptional circumstances (e.g. children moved outside the UK, unaccompanied Asylum Seeking young people, children coming to the UK independently) data must be transferred outside of the UK details will be documented of how appropriate safeguards will be put in place. Transferring personal data outside the UK comes with the responsibility of following the relevant rules and safeguards to facilitate such transfers. Please refer to the available ICO guidance and checklist here. Advice from the DPO will be required for any potential transfers.

8 Review

The arrangements held within this document will be reviewed by the Strategic Child Exploitation Group, initially after six months and then annually thereafter.

9 Ending the agreement

Any party wishing to end this agreement will be required to give 28 calendar days' notice in writing to the Strategic Child Exploitation Group. During this time the Group will be convened to review the implications of the termination.

10 Signatories

Each organisation should identify who is the most appropriate post holder within their agency to sign the ISA 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 ISA.

By signing this ISA, all signatories acknowledge and accept the requirements placed upon them and others within their organisations by the Tier 1 Overarching Safeguarding Children ISA and this Tier 2 Harm Outside the Home ISA and their responsibilities under data protection legislation.

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:
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:
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:
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:
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:
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:
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: Rachel Farnham
Role: Head of Children's Social Care
Email: Rachel.farnham@durham.gov.uk
Signature:
Date signed:
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:
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: Katherine Noble
Role: Medical Director and Caldicott Guardian
Email: Katherine.Noble@neas.nhs.uk
Signature:
Date signed:
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:
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:
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 - 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