



Information  
Sharing Agreement

Between

Derby City Council

And Statutory Partners who are called the

***Derby and Derbyshire Safeguarding Children Partnership***

Version 2.6

Document owner	M Sobey
Document author and enquiry point	
Document authoriser	
Date of document	09 September 2019
Version	2.6
Document classification	Official
Document distribution	Derby and Derbyshire Safeguarding Children Partnership
Next document review date	09.09.2021

## Contents

1. List of Partners to the Agreement .....	3
a) Partnership – Statutory Partners and joint Controllers .....	3
b) Further relevant agencies for the purposes of the section 16E(3) Children Act 2004 .....	3
2. Background and Scope of Agreement .....	4
3. Information to be shared .....	4
4. Purpose of Information sharing .....	5
1) Case Reviews (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning Reviews) .....	5
2) Quality Assurance Audits .....	6
3) Learning and Organisational Development .....	7
4) Reviewing Child Deaths .....	7
5. General DDSCP Information Processing .....	8
6. Lawful Basis for information sharing .....	9
“16H Information .....	9
7. Information to be shared .....	12
8. Exchange of information .....	13
9. Terms of use of the information .....	14
10. Data quality assurance .....	15
11. Data retention, review and disposal .....	15
12. Access and security .....	17
13. Data Protection Impact Assessment .....	18
14. Liability .....	18
15. Rights of the data subject .....	18
Right of access .....	18
Right to rectification .....	19
Right to restrict processing .....	19
Right to object .....	19
Rights related to automated decision-making including profiling .....	20
Right to be forgotten/to withdraw consent .....	20
Right to have data transferred .....	21
16. Management of the Agreement .....	21
17. Signatories .....	24
Appendix A Definitions .....	25

## **1. List of Partners to the Agreement**

This is a data sharing agreement between Derby City Council, its statutory partners who are members of the Derby and Derbyshire Safeguarding Children Partnership relating to the sharing of personal information.

### **a) Partnership – Statutory Partners and joint Controllers**

- 1) Derby City Council
- 2) Derbyshire County Council
- 3) Derbyshire Constabulary
- 4) Derby and Derbyshire Clinical Commissioning Groups
- 5) Tameside and Glossop Clinical Commissioning Group

### **b) Further relevant agencies for the purposes of the section 16E(3) Children Act 2004**

- 1) Police and Crime Commissioner for Derbyshire
- 2) Derbyshire Healthcare Foundation Trust
- 3) Derbyshire Community Health Service Foundation Trust
- 4) Chesterfield Royal Hospital Foundation Trust
- 5) University Hospitals of Derby and Burton NHS Foundation Trust
- 6) Derbyshire Health United
- 7) East Midlands Ambulance Service
- 8) GP's
- 9) Derbyshire Leicester Nottingham and Rutland Community Rehabilitation Company
- 10) National Probation Service Education
- 11) Children and Family Court Advisory Support Service (CAFCASS)
- 12) Independent lay members
- 13) Voluntary sector
- 14) Community Safety Housing providers
- 15) Chesterfield Borough Council
- 16) Derbyshire Fire and Rescue Service

It will be the responsibility of each party to:

- 1) Have realistic expectations on information sharing
- 2) Maintain standards in respect of information sharing
- 3) Have processes in place to control the flow of information
- 4) Meet Data Protection Act 2018 requirements

## 2. Background and Scope of Agreement

The objective of this agreement is to facilitate lawful and secure information sharing between members of the Derby and Derbyshire Safeguarding Children Partnership to support the work they do to keep the children and young people of Derbyshire safe.

The agreement takes into account the effect of relevant legislation, statutory guidance and common law, upon the way in which information is shared and used.

The relevant legislation is set out in the statutory guidance issued by the DfE called 'Working Together to Safeguard Children' (2018). Partners to this agreement are also expected to comply with the General Data Protection Regulation, the Data Protection Act 2018, the Human Rights Act 1998 and common law duties of care and confidentiality in conjunction with this guidance.

## 3. Information to be shared

Information sharing carried out under the legal framework contained in the Section 16H Children Act 2004 provides the legal basis for sharing the information with and on behalf of the Derby and Derbyshire Safeguarding Children Partnership.

### **“16H Information**

- 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 or 16F, 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 Derby and Derbyshire Safeguarding Children Partnership will process information for the following five purposes

1. Case Reviews (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning Reviews)

2. Quality Assurance Audits
3. Learning and Organisational Development
4. Reviewing Child Deaths
5. General DDSCP Information Processing

The data will include Personal data and Sensitive personal data. Personal data may be used for the purpose of quality assurance audit where appropriate. Where possible and appropriate this will be anonymised and pseudonymised.

It should be noted that the circumstances and details of each case will likely be so specific that the application of a pseudonym may not serve to protect identity in some circumstances, and consideration of this will be undertaken on a case by case basis.

## **4. Purpose of Information sharing**

The Derby and Derbyshire Safeguarding Children Partnership will process information for the following four purposes

### **1) Case Reviews (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning 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.

The purpose of information sharing is to enable the safeguarding partners to carry out their statutory function to implement local and national learning including from serious child safeguarding incidents. (Statutory Guidance: Working Together to Safeguard Children Page 73).

The information shared between partners covers criminal, health and social care information, including personal and special categories of data relevant to safeguarding case being reviewed.

The (National) Child Safeguarding Practice Review Panel may require the Derby and Derbyshire Safeguarding Partnership to provide information to them under the 16D Information Children Act 2004(as amended). This will relate, in the main, to Rapid Reviews, Child Safeguarding Practice Reviews and Serious Case Reviews which report cases of children who have died or been seriously harmed by abuse and neglect locally.

The process for undertaking local child safeguarding practice reviews will be managed by two partnership groups in Derby and Derbyshire areas and comply with national guidance.

The following DDSCP business team members will have responsibility for processing information in relation to case reviews. In order to achieve this they will have access

to the Children's Management System in Derby (Liquid Logic) and Derbyshire (Mosaic):

- Partnership Manager
- Safeguarding Practice Manager
- Business Services Officer (Child Safeguarding Practice)
- Business Services Officer (Minutes and QA)

## 2) Quality Assurance Audits

The purpose of information sharing is to enable the safeguarding partners to carry out their statutory function to quality assure local practice to determine whether:

- children are safeguarded and their welfare promoted
- partner organisations and agencies collaborate, share and co-own the vision for how to achieve improved outcomes for vulnerable children
- organisations and agencies challenge appropriately and hold one another to account effectively
- there is early identification and analysis of new safeguarding issues and emerging threats
- learning is promoted and embedded in a way that local services for children and families can become more reflective and implement changes to practice
- information is shared effectively to facilitate more accurate and timely decision making for children and families

(Statutory Guidance: Working Together to Safeguard Children Page 74).

The process for undertaking local quality assurance audit activity will be managed by two partnership groups in Derby and Derbyshire areas and comply with national guidance.

*The information shared between partners covers criminal, health and social care information, including personal, sensitive and special categories of data relevant to safeguarding case being reviewed.*

The following DDSCP business team members will have responsibility for processing information in relation to quality assurance audit and activity. In order to achieve this they will have access to the Children's Management System in Derby (Liquid Logic) and Derbyshire (Mosaic):

- Partnership Manager
- Safeguarding Practice Manager
- Strategic Quality Assurance Officer
- Vulnerable Children and Young People Development Officer
- Policy, Procedure and Regulation Officer
- Business Services Officer (Child Safeguarding Practice)
- Business Services Officer (Minutes and QA)

### **3) Learning and Organisational Development**

The purpose of learning and organisations development is to enable the safeguarding partners to carry out their statutory function to promote and embed learning in a way that local services for children and families can become more reflective and implement changes to practice.

(Statutory Guidance: Working Together to Safeguard Children Page 74).

Staffs compliance with mandatory national training is monitored throughout partner and relevant agencies on a routine basis, and is reviewed as part of the learning from quality assurance audits. The purpose of information sharing is to enable the professionals and volunteers who work for safeguarding partners to reaffirm the importance of effective training which can be accessed via the creation of an online training account to book their training courses and access training materials

The process for promoting and embedding learning will be managed by a single partnership group across Derby and Derbyshire areas and comply with national guidance.

The following DDSCP business team members will have responsibility for processing information in relation to Learning and Organisational Development:

- Safeguarding Practice Manager
- Senior Learning and Organisational Development Officer
- Learning and Organisational Development Officer
- Business Services Officer (Training)

### **4) Reviewing Child Deaths**

The responsibility for ensuring child death reviews are carried out is held by 'child death review partners,' who are defined as the local authority for that area and any clinical commissioning groups operating in the local authority area.

Child death review partners will implement arrangements to review all deaths of children normally resident in the local area and, if they consider it appropriate, for any non-resident child who has died in their area.

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.

The processes for undertaking child death reviews will be managed by a single partnership group called the Child Death Overview Panel across Derby and Derbyshire areas and comply with national guidance

The Child Death Overview Panel 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: (Statutory Guidance: Working Together to Safeguard Children Page 95).

The information shared between partners covers criminal, health and social care information, including personal and special categories of data relevant to safeguarding case being reviewed.

The DDSCP business team may be requested to process information to respond to requests for information from the Child Death Overview Panel.

The following DDSCP business team members will have responsibility for processing information in relation to child death reviews. In order to achieve this they will have access to the Children's Management System in Derby (Liquid Logic) and Derbyshire (Mosaic):

- Partnership Manager
- Safeguarding Practice Manager
- Business Services Officer (Child Safeguarding Practice)
- Business Services Officer (Minutes and QA)

## **5. General DDSCP Information Processing**

The purpose of information sharing is to enable the safeguarding partners to carry out their statutory function to quality assure local practice to determine whether:

- children are safeguarded and their welfare promoted
- partner organisations and agencies collaborate, share and co-own the vision for how to achieve improved outcomes for vulnerable children
- organisations and agencies challenge appropriately and hold one another to account effectively
- there is early identification and analysis of new safeguarding issues and emerging threats
- learning is promoted and embedded in a way that local services for children and families can become more reflective and implement changes to practice
- information is shared effectively to facilitate more accurate and timely decision making for children and families

(Statutory Guidance: Working Together to Safeguard Children Page 74).

The following DDSCP business team members will have responsibility for processing information in relation to the functions of the DDSCP.

- Independent Chair of the DDSCP
- Partnership Manager



- Safeguarding Practice Manager
- Strategic Quality Assurance Officer
- Vulnerable Children and Young People Development Officer
- Policy, Procedure and Regulation Officer
- Senior Learning and Organisational Development Officer
- Learning and Organisational Development Officer
- Business Services Officer (Child Safeguarding Practice)
- Business Services Officer (Minutes and QA)
- Business Services Officer (Training)

## **6. Lawful Basis for information sharing**

Information sharing carried out under the legal framework contained in the Section 16H Children Act 2004 provides the legal basis for sharing the information with and on behalf of the Derby and Derbyshire Safeguarding Children Partnership.

### **16H Information**

(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 or 16F, 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 Derby and Derbyshire Safeguarding Children Partnership will process information for the following five purposes

1. Case Reviews (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning Reviews)
2. Quality Assurance Audits
3. Learning and Organisational Development
4. Reviewing Child Deaths
5. General DDSCP Information Processing

The data will include Personal data and Sensitive personal data. Personal data may be used for the purpose of quality assurance audit where appropriate. Where

possible and appropriate this will be anonymised and pseudonymised. Audit findings will be anonymised.

Under the General Data Protection Regulation and the Data Protection Act 2018 the legal bases for sharing information between the Partners under this agreement have been identified as:

**6(1)(a)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

**6(1)(b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

**6(1)(c)** processing is necessary for compliance with a legal obligation to which the controller is subject;

**6(1)(d)** processing is necessary in order to protect the vital interests of the data subject or of another natural person;

**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

In the case of Special Categories of Personal Data, partners must also meet Article 9 condition by virtue of subsection 2 (a), (b), (c), (g) or (h):

The processing is necessary:

- Article 9(2) (b) for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field 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) (c) in order to protect the vital interests of the data subject or another natural person in a case-
  - where the data subject is physically or legally incapable of giving consent;
- Article 9(2) (g) 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 9(2) (h) for the purposes of preventive or occupational medicine, for the assessment of the 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 of Article 9.

Access to records may be also be undertaken under the provisions of the GDPR, Data Protection Act 2018, and the Access to Health Records Act 1990 (in the case of the records of the deceased individuals).

The public tasks based on the public interest and legal obligations arise from the following provisions:

The Working Together to Safeguard Children 2018 statutory guidance states which sections in the following Acts the above legal bases and conditions relate to:

- Children Act 1989
- Children Act 2004
- Education Act 1996
- Education Act 2002
- Education and Skills Act 2000
- Legal Aid, Sentencing and Punishment of Offenders Act 2012
- Police Reform and Social Responsibility Act 2011
- Childcare Act 2006
- Crime and Disorder Act 1998
- Housing Act 1996
- Safeguarding Vulnerable Groups Act (SVGA) 2006
- Department of Education Guidance with regards to:
  - 1) Safeguarding children Department for Education, Home Office, Ofsted, Department of Health and Social Care, Ministry of Housing, Communities & Local Government, Care Quality Commission, Department for Digital, Culture, Media & Sport, and Foreign & Commonwealth Office
  - 2) Safeguarding Children in whom illness is fabricated or induced Department for Education, Department of Health and Social Care and Home Office
  - 3) Safeguarding children who may have been trafficked Department for Education and Home Office
  - 4) Safeguarding strategy - unaccompanied asylum seeking and refugee children
  - 5) Statutory visits to children with special educational needs and disabilities or health conditions in long-term residential settings Department for Education and Department of Health and Social Care
  - 6) The Child Safeguarding Practice Review and Relevant Agency (England) Regulations 2018
  - 7) The prevent duty: for schools and childcare providers
  - 8) United Nations Convention on the rights of the child
- Guidance issued by other government departments and agencies - Criminal exploitation of children and vulnerable adults: county lines Home Office
- Guidance issued by external organisations with regards to
  - 1) Child maltreatment: when to suspect maltreatment in under 18s NICE
  - 2) Child protection and the Dental Team British Dental Association
  - 3) Children's rights and the law - Children's Rights Alliance for England
  - 4) Cyberbullying: Understand, Prevent, Respond – Guidance for Schools Childnet International
  - 5) How we protect children's rights – Unicef

## 7. Information to be shared

This agreement enables partners to share the following personally identifiable information, for the purpose outlined in 3, relating to relevant children, their family members and relevant significant others with the DDSCP and partners to this agreement, where relevant to do so.

- Name
- Address
- Date of Birth/Age
- Gender
- Ethnicity

Also, if necessary, this agreement enables relevant information about the above individuals held by local authorities, the police, probation agencies, health agencies and other agencies who are partners to this agreement to be shared between them for the same purpose.

Although this is not an exhaustive list, examples of relevant information may include:

- Personal and sensitive information which identifies the alleged victim(s) or alleged perpetrator(s) of abuse or neglect e.g. name, date of birth, address; sensitive information about the alleged victim(s) or alleged perpetrator(s) of abuse or neglect e.g. gender, religion, ethnicity
- Reasons for concerns and details of the alleged concerns e.g. type of abuse, location of abuse, levels of risk or urgency.
- Information about the physical and or mental health of the alleged victim(s) or alleged perpetrator(s) e.g. mental capacity, communication needs
- Reports of any medical or social care assessments or examinations undertaken as part of the safeguarding procedures e.g. eligibility for community care, psychiatric assessment
- Personal data which identifies professionals involved with the alleged victim(s) or alleged perpetrator(s)
- Personal data which identifies other people who may be at risk
- Historical information held in records about the alleged victim(s) or alleged perpetrator(s) that may be relevant to the current concern
- Name and contact details of the referrer (unless they have stated they wish to remain anonymous and this anonymity would not have a detrimental impact upon the protection process)
- Name of employer or organisation if the concern relates to a paid worker or volunteer of a service provider

The agreement also concerns aggregated data (e.g. statistics) which may be shared. In these situations, anonymised information should be used.

DDSCP may share the personally identifiable data obtained from partners with Independent Report Authors commissioned by the Partnership, under confidentiality agreements compliant with data protection legislation to write reports.

DDSCP will only share anonymised and/or pseudonymised data with national bodies such as OFSTED when sharing information on reviews. All reviews published in public domain will be anonymised.

Information shared may also be used for planning and research purposes by partner organisations. This information must be anonymised or pseudonymised if used for these purposes as this will be a secondary use of the information.

If large volumes of data are provided for research and/or planning by partner organisations, as a matter of courtesy the outcome of that research/planning should be provided to the organisation(s) supplying the data.

Derbyshire County Council and Derby City Council are under a duty to protect the public funds they administer and to this end may use information provided by partners for the prevention and detection of fraud however, only with the prior agreement of the partners who have provided the information.

## **8. Exchange of information**

Documents not containing personal or commercially sensitive data can be shared by whatever is considered to be an appropriate medium by the partners.

Documents containing personal data or commercially sensitive data will only be shared by secure methods;

- Web portals, such as those used by regulatory bodies (Ofsted) may be used following verification that industry standard security and authenticated access is in place
- Secure email solutions with industry standard security e.g. Transfer Layer Security Compliant Email, Egress
- Encrypted files with industry standard security

The DDSCP business team members will use secure email or an alternative secure method as described above sharing personal or special categories of data.

In all circumstances where independent consultants are involved in the work of the DDSCP, any communications with them will be via secure email. Due diligence checks will take place to ensure that these consultants have appropriate email security in place, and a relevant contractual arrangement which stipulate confidentiality expectations will be in place prior to commencement. Any external consultant will be expected to maintain the same standards of behaviours as employed staffs, and this will include training requirements.

The DDSCP business team members will provide Encrypted Memory Sticks for the use by associate Training pool members to deliver content on training courses. The information held on encrypted memory sticks will not include personal or sensitive information.

Partners can either include the operational data sharing arrangements under this agreement with Partner agencies as an appendix to this agreement or create separate local information sharing agreements with Partner agencies. An example of a local data sharing agreement is the Derbyshire Constabulary – Information Sharing Agreement for Working Together to Safeguard Children.

## **9. Terms of use of the information**

Information will only be used for the specified purpose. The Derby and Derbyshire Safeguarding Children Partnership will process information for the following five specified purposes

- 1) *Case Reviews (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning Reviews)*
- 2) *Quality Assurance Audits*
- 3) *Learning and Organisational Development*
- 4) *Reviewing Child Deaths*
- 5) *General DDSCP Information Processing*

Where it is reasonably determined that further information is necessary to fulfil statutory duties and/or other requirements this Agreement will be reviewed in full or in part as appropriate.

Partners will ensure information shared under this agreement is reviewed regularly in accordance with their own data quality policies and procedures.

Partners recognise their collective responsibilities as joint controllers.

Whenever possible personal data should be appropriately minimised this may be through pseudonymisation, anonymisation or just limiting the amount of data processed or shared.

The parties will only store “person identifiable” data shared between all partners on secure systems which can only be accessed by a restricted number of appropriate staff with appropriate security safeguards.

The parties will use the data supplied for the purposes stated and will not pass such data to third party organisations outside the remit of specified partners in agreement without prior written consent from the parties to this agreement.

It is also prohibited under this agreement for sub-processors to be used without the prior consent of the Controller(s).

Where applicable all parties will comply with their obligations under the Freedom of Information Act 2000. Either party may consult with the other party/parties if necessary if requests relate to information shared but will remain responsible for responding to the request.

The parties will ensure that Privacy Notices are available on organisational websites, and issued to all data subjects in accordance with the information commissioners' guidance & the standards set out in the Data Protection Act 2018. As part of the mobilisation of this agreement, the partner to DDSCP will share the content of their privacy notices to ensure consistency of message and data subject rights procedures.

## 10. Data quality assurance

Information shared will be adequate, relevant, accurate and up to date.

- All parties to this agreement will adhere to their internal data quality policies and procedures when storing, sharing and updating information.
- Information shared under this agreement discovered to be inaccurate, out-of-date or inadequate for the purposes of this agreement should be notified to the source Partner Controller; who will be responsible for correcting the data and notifying all the parties within 2 working days, where information is discovered to be inaccurate, out-of-date or inadequate for the purpose.
- All parties must make any relevant amendments as required.

## 11. Data retention, review and disposal

Partners will make sure that all information shared under this agreement, regardless of format, will be destroyed in accordance with their own local policies and procedures relating to retention and disposal of record to ensure compliance with the General Data Protection Regulation, Data Protection Act 2018 and any subsequent legislation.

Partners will ensure that data retained is not kept for any longer than is necessary and will be destroyed in accordance with their own local policies and procedures relating to retention and disposal of record to ensure compliance with the General Data Protection Regulation, Data Protection Act 2018 and any subsequent legislation.

The Derby and Derbyshire Safeguarding Children Partnership will retain information for the five specified purposes following the following standards

### 1) **Case Reviews** (Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, Serious Incident Learning Reviews)

All records relating to Rapid Reviews, Serious Case Reviews, Child Safeguarding Practice Reviews, and Serious Incident Learning Reviews including the final report

- Contains personal information
- Impact level Official – Sensitive
- Legal & business requirement

- Retention - Retain from date of report for 15 years in accordance with Retention Guidance for Local Authority 2013 or as amended by statute and government guidance.

## **2) Quality Assurance Audits**

All records relating to audit including the final report

- Contains personal information
- Impact level Official – Sensitive
- Legal & business requirement
- Retention - Retain from date of report for 15 years in accordance with Retention Guidance for Local Authority 2013 or as amended in by statute and government guidance.

## **3) Learning and Organisational Development**

All records relating to the management of the delivery of learning and organisational development including training of the Derby and Derbyshire Safeguarding Children Partnership.

- Contains personal information
- Impact level Official
- Business requirement
- Retention - Retain from year records created for 4 years in accordance with Retention Guidance for Local Authority 2013 or as amended in by statute and government guidance.

## **4) Reviewing Child Deaths**

All records relating to Child Death Reviews

- Contains personal information
- Impact level Official – Sensitive
- Legal & business requirement
- Retention - Retain from date of report for 15 years in accordance with Retention Guidance for Local Authority 2013 or as amended in by statute and government guidance.

## **5) General DDSCP Information Processing**

All records relating to the constitution and management of the Derby and Derbyshire Safeguarding Children Partnership

- Contains personal information
- Impact level Official
- Business requirement



- Retention - Retain from year records created for 4 years in accordance with Retention Guidance for Local Authority 2013 or as amended in by statute and government guidance.

## **12. Access and security**

Ensure that measures are in place to prevent any breach their common law duty of confidentiality. The partners to this agreement have policies and systems in place to ensure information held on its information systems is held securely and in compliance with the security requirements of the General Data Protection Regulation, Data Protection Act 2018 and any subsequent legislation applicable to the processing of the personal information shared under this agreement.

Each party will make sure they take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In particular, each party must make sure they have procedures in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- deter deliberate compromise or opportunist attack
- dispose of or destroy the data in a way that makes reconstruction unlikely
- promote discretion to avoid unauthorised access.
- be ready and prepared to respond to any breach of security swiftly and effectively and all parties must ensure that any breaches are reported to the Controller within two working day.
- report any breaches to the relevant Controller immediately – not exceeding two working days.
- maintain a record of personal data and processing activities regarding the data.

Access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.

All Derby City Council and staff from all other parties to this agreement must comply with data protection legislation as part of their employment contract.

Derby City Council and all other parties to the agreement affirm that they have policies and systems in place to ensure information held on its information systems is held securely and in compliance with industry security standards and legislation.

## **13. Data Protection Impact Assessment**

Under the new EU General Data Protection Regulations a Data Protection Impact Assessment (DPIA) is an assessment made prior to processing of the impact of the processing on the protection of personal data, will be mandatory in certain circumstances. This will be the case where the processing is likely to result in a high risk to the rights and freedoms of individuals.

## **14. Liability**

Under the Data Protection Act (DPA) 2018 the data subjects are able to take action against both Controllers and Processors and potentially claim damages where they have suffered material or immaterial damage as a result of an infringement of obligations under the DPA ("Compensation"). Under the DPA the Information Commissioner's Office can also fine a processor or a controller in relation to any breaches of the DPA.

In the event that the Controller or the Processor (for the purposes of this clause: "Party A") is ordered by a Court/Tribunal to pay Compensation to a Data Subject or is required to pay a fine by the Information Commissioner's Office, to the extent that such Compensation has arisen as a result of the act, negligence, omission or default of the other party ("Party B"), Party B shall indemnify Party A in respect of that element of the Compensation.

## **15. Rights of the data subject**

Please note that all rights as described below are qualified rights, and where safeguarding legislation is the basis for processing, a consideration on a case by case basis will be undertaken by the relevant data controller.

### **Right of access**

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice (see 'Supplementary information' below).

If the right is successfully engaged the Controller will confirm in writing and ensure that the data is deleted within one month of the request. The Processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

### **Right to rectification**

Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

If the right is successfully engaged the relevant Controller will provide written instructions to confirm in writing and ensure that the relevant data is amended within one month of the request. The party/parties will assist the relevant Controller in their investigation and will comply with any instructions in regards to amending the personal data within a period of 5 working days.

### **Right to restrict processing**

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the ways that an organisation uses their data.

If the right is successfully engaged the Controller will confirm in writing and ensure that the data is restricted within one month of the request. The Processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

### **Right to object**

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.

If the right is successfully engaged the Controller will confirm in writing and provide written instructions to the other party/parties to ensure that the data is deleted within one month of the request. The parties will comply with any instructions in regards to processing the personal data 5 working days.

## **Rights related to automated decision-making including profiling**

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The parties must comply with the relevant GDPR provisions regarding all automated individual decision-making and profiling.

If a challenge is successfully engaged the Controller will provide written instructions to ensure that the data is deleted within one month of the request. The parties will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## **Right to be forgotten/to withdraw consent**

Under the DPA the data subject will have the right to withdraw and revoke their consent at any time. The data subject/s therefore has a right to request that their data be removed or deleted in certain circumstances, namely if one of the following conditions is met:

- the personal data is no longer necessary or relevant in relation to the purpose for which it was original collected;
- the individual specifically withdraws consent to processing (and if there is no other justification or legitimate interest for continued processing);
- personal data has been unlawfully processed, in breach of the DPA;
- the data must be erased in order for a controller to comply with legal obligations (for example, the deletion of certain data after a set period of time).

However the Controller must also balance any request against the public interest. They must take into account the exceptions to the right of erasure and make a decision whether to comply with the request.

If the right is successfully engaged the Controller will provide written instruction to ensure that the data is deleted within one month of the request. The parties will comply with any instructions to delete personal data in such circumstances within five working days.

## Right to have data transferred

Under the DPA an individual has the right to have their personal data transferred where:

- personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The DDSCP business team will process data of an individual in the three above circumstances specifically in relation to data held by individuals who have registered for courses using the online booking system.

The DDSCP business team will process requests for data to be transferred with the external provider who operates the online booking system (this provider is to be confirmed on completion of the procurement process and will be subject to the relevant data sharing and contractual arrangements being in place.)

In response to such a request the parties will provide personal data in a structured, machine readable format. The information will be provided free of charge within one month of the request.

If the request is complex or a number of requests are received the time limit for compliance may be extended by two months and the individual must be informed within one month of receipt of the initial request as to why the extension is being applied.

The parties will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## 16. Management of the Agreement

Any complaints or breaches of the agreement will be dealt with as set out in the clauses of the Contract for the provision of services.

This agreement will be reviewed every two years, or at the time of any material changes to the processing.

*As some of the data shared under this agreement is deemed as special category data as defined by the Data Protection Act 2018 it should be handled in accordance with the information management classification for this type of data in each partner organisation which should cover:*

- *physical and electronic security measures*

- *ensuring only appropriate employees having access to the information in line with requirements set out in sections 2, 3 and 4 of this document.*

All complaints or breaches relative to this agreement will be notified to the designated Data Protection Officer of the relevant organisation in accordance with their respective policy and procedures.

Each party will make sure that all breaches of agreement, internal discipline, security incidents or malfunctions will be managed in accordance with their own local policies and procedures to ensure compliance with the Data Protection Act 2018. Should any such incident arise, the relevant data controller will inform all other parties to this agreement.

All parties to this Agreement will undertake to indemnify the other against any legal action arising from any breach of this Agreement by any person working for or on behalf of its own organisation.

The data may only be shared with the parties to this agreement and will not be shared with any other third party or any other Authority without the explicit written consent of the Controller.

Any party who receives a request for information under the subject access provisions of the Data Protection Act 2018 or Freedom of Information Act 2000, must progress it in accordance with the statutory obligations.

The parties agree to undertake reasonable efforts to liaise with the other party or parties, as necessary to agree on relevant exemptions from disclosure.

Any Processor will ensure that they refer any statutory requests to the Controller within two working days.

The Information Sharing Agreement will cover the period 29/09/2019 to 31/03/2021 It will be reviewed every 24 months thereafter, or at the time of any material changes to the processing.

Any partner organisation can suspend the Information Sharing Agreement for a preliminary period of 30 days, if they feel that statutory compliance or security has been seriously breached.

Notification of termination and/or completion by either party must be given in writing with at least 30 days' notice.

The following officers will have responsibility for carrying out the obligations in this Agreement on behalf of the parties and are the initial point of contact for any queries relating to this Agreement or the information shared under it.


## Data Protection Officers

On behalf of Derby City Council	
Name of officer	<b>Sinead Booth</b>
Position	<b>Data Protection Officer</b>
Telephone number	<b>01332 643318</b>
Email	<b>Sinead.booth@derby.gov.uk</b>
On behalf of <i>Derbyshire County Council</i>	
Name of officer	<b>Simon Hobbs</b>
Position	<b>Deputy Director of Legal Services/Data Protection Officer</b>
Telephone number	<b>01629 538306</b>
Email	<b>simon.hobbs@derbyshire.gov.uk</b>
On behalf of <i>Derbyshire Constabulary</i>	
Name of officer	<b>Abby Turner</b>
Position	<b>Head of Information Management</b>
Telephone number	<b>0300 1228756</b>
Email	<b>Abby.turner@derbyshire.police.pnn.uk</b>
On behalf of <i>Derby and Derbyshire Clinical Commissioning Group</i>	
Name of officer	<b>Steve Lloyd</b>
Position	<b>Medical Director and DPO</b>
Telephone number	<b>01246 514051</b>
Email	<b>stevenlloyd@nhs.net</b>
On behalf of <i>Tameside and Glossop Clinical Commissioning Group</i>	
Name of officer	<b>Sandra Stewart</b>
Position	<b>Director of Governance and Pensions</b>
Telephone number	<b>0161 342 2711</b>
Email	<b>Sandra.stewart@tameside.gov.uk</b>

## 17. Signatories – Names to be added

Authorised signatory for and on behalf of Derby City Council	
Print name	Jasmine Nembhard-Francis
Position	Head of Service Children Quality Assurance
Date	02/10/19
Authorised signatory for and on behalf of Derbyshire County Council	
Print name	Chris Newton
Position	Head of CS Information and ICT
Date	16/09/2019
Authorised signatory for and on behalf of Derbyshire Constabulary	
Print name	Matt Thompson
Position	D/Supt, Head of Public Protection
Date	19/09/2019
Authorised signatory for and on behalf of Derby and Derbyshire Clinical Commissioning Group	
Print name	Brigid Stacey
Position	Chief Nursing Officer
Date	17/09/2019



Authorised signatory for and on behalf of <i>Tameside and Glossop Clinical Commissioning Group</i>	
Print name	Gill Gibson
Position	Director of Quality and Safeguarding
Date	16/09/19

## Appendix A Definitions

### Personal Data

Data which relates to a living individual who can be identified;

a) from those data; or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the Controller.

And includes any expression of opinion about the individual and any indication of the intentions of the Controller or any other person in respect of the individual.

It should also be noted that the definition of personal data is extended to include IP addresses.

### Sensitive or Special Categories of Personal Data

Sensitive or Special Categories of Personal Data means personal data consisting of;

- a. racial or ethnic origin of the data subject
- b. political opinions
- c. religious beliefs of other similar beliefs
- d. trade union membership
- e. physical or mental health
- f. sexual life
- g. commission of alleged commission of offences

- h. any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
- i. Genetics
- j. biometrics (where used for ID purposes)

**Data Subject** - means an individual who is the subject of personal data.

**Controller** – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Processor** - means any person (other than an employee of the controller) who processes the data on behalf of the controller.

**Processing** – means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.