Direct Care Information Sharing Agreement

Health services for school age children not educated in a school setting or children who are not on a school roll and therefore missing education.

PURPOSE	LPT provide a range of services to children throughout Leicestershire County. Where appropriate the services are delivered through schools, however, the remit of LPT is not limited to children who are educated in a school setting. The local authority gathers information about children that are not being educated in a school setting. This includes children educated at home or who are missing education. This agreement covers data to support the provision of health services to school aged children whose parents have elected to educate at home and those children who are not on a school roll and therefore are missing education.

Partners
• Rutland County Council (RCC) • Leicestershire Partnership Trust (LPT)

Date agreement comes into force:	When signed

Date of Agreement Review:	A year after signature then 2 yearly thereafter

Agreement Owner:	Senior Information Risk Owners (SIROs) of partners set out above

Agreement Drawn up by:	Kevin Turner / Leicestershire County Council

Protective Marking:	OFFICIAL

VERSION RECORD

Version No.	Amendments Made	Authorisation	Date
0.1	Initial draft	SB / RCC	14/09/2021

1. Policy Statements and Purpose of this Information Sharing Agreement

1.1 Purpose and Justification for Information Sharing

LPT provide a range of services to children throughout Leicestershire County. Where appropriate the services are delivered through schools, however, the remit of LPT is not limited to children who are educated in a school setting.

The local authority gathers information about children that are not being educated in a school setting. This includes children educated at home or who are missing education.

This agreement covers data to support the provision of health services to school aged children whose parents have elected to educate at home.

The information will be shared with LPT to enable them to contact families to offer appropriate services such as immunisation. It is up to the families to decide whether to take up the services.

2. Governance

This Agreement sits under the over-arching Leicester, Leicestershire & Rutland (LLR) Information Sharing Protocol (ISP) agreed in July 2019, which lays out broad principles for the sharing of information.

It complies with the Information Commissioner's revised Data Sharing Code of Practice (a statutory code of practice made under section 121 of the Data Protection Act 2018.

Where required by UK GDPR, a Data Protection Impact Assessment will be carried out on information sharing activity within this ISA.

If the data sharing is of a type likely to result in a high risk to children's rights and freedoms, a DPIA is compulsory.

This ISA demonstrates compliance with the accountability principle under GDPR Article 5(2).

3. Lawful and Fair processing

This Agreement has been developed to achieve the purpose and business objectives as set out in Section 1 above. It is the intention that all aspects of information exchange and

disclosure relating to this Agreement shall comply with relevant legislation that protects personal data.

A lawful basis may be provided by common law, statute or legal precedent supported by Home Office guidance or professional/executive bodies, e.g. Dept of Health, Association of Chief Police Officers, Dept of Education, etc. Identifying a lawful basis will enable partners to defend a challenge with regard to current data protection legislation and/or the Human Rights Act 1998 and is necessary for compliance with the first principle of data protection legislation.

Appendix A identifies statutory gateways for information exchange that apply to the partner agencies for the purpose of this agreement.

3.1 General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18)

The disclosure must be compliant with the GDPR and DPA18 and the ways in which this information sharing will comply with the principles is set out in **Appendix B**. Each data controller is responsible for putting these steps in place and for any breaches of this Agreement which occur through failure to do so.

3.2 Human Rights Act 1998 (HRA)

The HRA applies to all public authorities and parties to this agreement endeavour to ensure that the principles of the HRA are enshrined in their actions. Proportionality has been identified as the key to Human Rights compliance. This means striking a fair balance between the rights of the individual and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law:-

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

Any disclosure must therefore be covered by one of these categories.

The personal data to be shared to implement the purpose has been identified as necessary to promote public safety, to prevent crime and disorder and the protection of health by early identification of vulnerability and need on public services. This will also include those individuals at high risk of harm for example where an individual is subject to domestic abuse which breaches Article 3, prohibition of torture and potentially Article 2, the right to life.

The minimum amount of personal data that is required to achieve the purpose will be shared in pursuance of the purpose which is proportionate and justifies the interference with the Article 8 rights of the data subjects.

3.3 Common Law Duty of Confidence

This applies when an individual provides information with the expectation that it will be kept in confidence and not disclosed. If the individual subsequently gives consent to the disclosure, it enables agencies to disclose information without further justification. If the individual does not consent, then a public interest test[1] should be undertaken to assess the impact of disclosure on the suspect/offenders/victim information against the harm which might be caused to a child or a vulnerable adult if the information is not disclosed.

3.4 Equality

Equality issues have been considered with regard to this ISA and all partners will ensure that information is shared in compliance with Equality and Diversity legislation and their internal Equality and Diversity policies.

3.5 Caldicott Principles

The Caldicott Committee (which reported in 1997) recommended a series of principles that should be applied when considering whether confidential information. Particularly in health and social care services, should be shared. The principles have been developed with the aim of establishing the highest practical standards for handling confidential information. They apply equally to all routine and ad hoc flows of service users/patient information whether clinical or non-clinical, in manual or electronic format. Any sharing undertaken under this Agreement must consider these principles. The principles are:

- **Justify the purpose(s) for using confidential information**
  Every proposed use or transfer of service user or patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

- **Only transfer/use service user or patient-identifiable information when absolutely necessary**
  Service user or Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for service users/patients to be identified should be considered at each stage of satisfying the purpose.

- **Use the minimum identifiable information that is required**
  Where use of service user/patient-identifiable information is considered to be essential, the inclusion of each individual item should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- **Access should be on a strict need to know basis**

[1] **Public Interest Test.** When applying the test, the public authority is simply deciding whether in any particular case it serves the interests of the public better to withhold or to disclose information.

Only those individuals who need access to service user/patient-identifiable information should have access to it. They should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

- **Everyone with access to identifiable information must understand his or her responsibilities**
  Action should be taken to ensure that those handling service user/patient-identifiable information, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect an individual's confidentiality.

- **Understand and comply with the law**
  Every use of service user or service user/patient-identifiable information must be lawful. Someone in each organisation handling service user or patient information should be responsible for ensuring that the organisation complies with legal requirements.

- **The duty to share information can be as important as the duty to protect service user or patient confidentiality.**
  For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

4 Information

4.1 Information to be shared

Personal data is information which relates to any living individual who can be identified from the data or from the data and other information held by the Controller.

Appendix A sets out the statutory gateways under which personal data may be exchanged for the purposes of this Agreement. Wherever possible only aggregated information should be shared so that individuals cannot be identified.

The personal data shared by Partners will be the minimum amount required and limited to what is necessary to achieve the Purpose set out in the Agreement. The personal data that will be shared by the Partners is listed in **Appendix C**.

4.1.1 Use of the Data and Limitations

This agreement covers data to support the provision of health services to school aged children whose parents have elected to educate at home and those children who are not on a school roll and therefore are missing education.

5 Further Use and Disclosure

The partners will not use the information shared under this ISA for any purpose other than that agreed in the 'Purpose' and will not further disclose any information without the written consent of the originating partner.

6 Data Quality

Partners will ensure as far as possible that the information which they supply is accurate and any information discovered to be inaccurate, out-of-date or inadequate for the purpose must be referred to the originating Partner, who will be responsible for

correcting that data. The originating Partner will also be responsible for notifying all other recipients of the information who must ensure that necessary corrections are made without delay. Appropriate records will be kept to record the sources of information to provide for this.

Where the receiving partners have difficulties matching that information with information already in their possession, the disclosing Partner will assist as far as possible to ensure that the correct information is data matched.

7 Responsibility for sharing this information

Each partner will identify a Designated Officer who will be authorised to process, extract, share and data match for the Purpose. This SPoC will ensure the Data they supply is accurate, relevant and limited to achieve the Purpose. The Designated Officer will be responsible for the management and compliance of this ISA.

Contact details are contained in **Appendix D**

8 Ownership

Where Partners jointly determine the purpose of the processing (e.g. multi-agency meetings, joint systems), Partners will be Joint Controllers in respect of the Agreement. This information sharing agreement meets GDPR Article 26's requirement to have an agreement in place for this processing.

Where Data is used for their own individual purposes (e.g. to provide services to individuals after identification via data matching or multi-agency meetings), and a Partner uses the information to the extend it determines the means and the purpose of processing, they will be Controllers in their own right; they will therefore be individually and legally liable for the processing it undertakes, and each will be responsible for complying with any statutory obligation.

Each Controller will be responsible for ensuring that the information is held and used securely in accordance with the Purpose, relevant legislation and this Information Sharing Agreement.

When Partners are joint controllers, they will ensure a data processing agreement is in place with any of their data processors which will detail the responsibilities and obligations of and obligations of the data processor.

9 How long will it be retained by the parties?

The data held by each of the Partners within its Information Management Systems for its own purposes as sole data controllers will be retained and disposed of in accordance with its own retention and disposal policy.

10 Security and Vetting

Each Partner has a legal responsibility under the Data Protection Legislation to ensure appropriate security measures are in place relating to the processing of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or dame using appropriate technical or organisational measures.

The data required for this agreement is personal data. For data matching purposes the data should be marked and or treated as OFFICIAL. More sensitive personal data discussed at multi-agency meetings e.g. criminal activity, health issues, should be considered to be "Official – Sensitive [Personal]" when applying the Government

security classifications requirements in **Appendix E** for those organisations that have implemented this scheme. If the organisation has not implemented this scheme, it should handle the data in accordance with its own security policies.

Any personal information shared under this ISA must only be accessible to and used by the partners' employees to whom it is disclosed to carry out the purpose stated in this agreement and it must not be further used or disseminated.

11 Audit

Each Partner must have an audit facility in place on their own systems used to provide data so that any access to the personal data shared under this ISA can be audited.

12 Breach of Personal Data

A Personal Data Breach is defined as as breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Partners will adhere to the following procedure if there is a breach of personal data by a Partner or a third party who has received information under this agreement. Examples of breaches include, but are not restricted to, the following:

- The loss, theft or misuse of data or information.
- The transfer or disclosure of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or the system.
- Changes to information or data or system hardware, firmware, or software characteristics without proper authorisation or consent.
- Unwanted disruption or denial of service to the system.
- The unauthorised use of the system for the processing or storage of data by any person.

The relevant Data Protection Officer (DPO) for each Partner is responsible for reporting high-risk breaches to the Information Commissioner Office (ICO) without undue delay, but no later than 72 hours after having become aware of the breach. Where such a breach presents a high risk to the rights and freedoms of the data subjects, the affected organisation must also inform the individual/s without undue delay.

All breaches, including those unlikely to result in a risk to the data subject, must be reported to the originating Partner(s). This must take place without undue delay in order for all relevant Partners to mitigate any ongoing risks to the data subjects.

All breaches will be recorded and investigated by the partners involved and Leicestershire Police will be consulted and determine whether any criminal investigation is required.

The contact details for the post holder who should be notified for each partner is recorded in the signatories table. The outcome and learning from any investigation will be circulated to all Partners.

Disciplinary action must be considered against any member of staff found to have been responsible for the breach by the employing Partner, with the Information Commissioner being notified of the breach and any action taken if the breach is serious. Partners will seek to ensure that consistency is applied in these matters.

13 Review of Information Sharing Agreements

This Agreement will initially be 12 months after signature and then 2-yearly unless legislation changes. The review may include a physical review to monitor adherence to the ISA.

Any partner may give reasonable written notice to the others requiring a review of any aspects of this agreement, which will take place at the earliest opportunity.

14 Suspension or termination of agreement

Unless there is a statutory obligation to share the data, any partner organisation can suspend this ISA for 45 days if security has been seriously breached and all signatories informed immediately. If necessary, steps will be taken to restrict access to the system as soon as possible.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this agreement, or their nominated representative. This meeting should take place within 14 days of any suspension.

Termination of, or withdrawal from, this Information Sharing Agreement should be in writing to all other Partner Organisations giving at least 30 days' notice.

For avoidance of doubt, termination or withdrawal from this ISA does not relieve the Partners from its statutory obligations in relation to the processing of personal data.

15 Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

Each partner organisation shall consider publishing this Agreement on its website and refer to it within its publication scheme.

All recorded information held by public sector agencies is subject to the provisions of the FOIA or the EIR. Information requests made under the FOIA or the EIR will be co-ordinated and responded to by the organisation receiving the request in relation to the whole of the information held that is relevant to the request. Even where there is no requirement to consult with third parties in responding to requests for information, the parties to this ISA will consult the parties from whom information originated or relates to and will consider their views to inform the decision-making process.

Nothing in this section shall prevent individual partner organisations from exercising their obligations and responsibilities under the FOIA or the EIR as they see fit.

16 Requests for Disclosure of Personal Information and Other Information Rights under the UK GDPR and DPA18

Subject Access Requests and other notices relating to a data subjects rights made under the UK GDPR and DPA18 will be co-ordinated and responded to by the organisation receiving the request and, where relevant, the fee. Even where there is no requirement to consult with third parties in responding to requests for information, the parties to this ISA will consider consulting the parties from whom information originated or relates to and will consider their views to inform the decision-making process.

Nothing in this section shall prevent individual partner organisations from exercising their obligations and responsibilities under the subject access provisions of the UK GDPR and DPA18 as they see fit.

17 Amendments

If there are any proposals to make key changes to this information sharing agreement, all signatories must be consulted. The agreed changes must be documented and included as an appendix to this ISA. Each signatory should record their agreement to the amendments.

18 Signatories

Each of the partners will sign the agreement. The signature on behalf of each partner shall be that of the Chief Officer or the SIRO for that organisation, or as per that Organisation's policy.

Partner Organisation	Information Security Contact Name &Number
LCC	Data Protection officer 01572 758165 dataprotection@rutland.gov.uk
LPT	Head of Data Privacy/Data Protection Officer 0116 2955296 LPT-DataPrivacy@leicspart.nhs.uk

Signatures

Rutland County Council

Name: Phillip Horsfield
Role: Deputy Director Corporate Services & SIRO
Email: dataprotection@rutland.gov.uk

Signature: 

Date of Signature: 15/09/2021

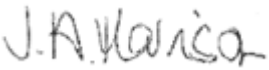
Leicestershire Partnership NHS Trust

Name: Janet Harrison

Role: Head of Service

Tel No.: 07789176169

Email: janet.harrison@leicspart.nhs.uk

Signature: 

Date of Signature: 15.09.2021

Appendix A: Health services for school age children not educated in a school setting – Legislative Framework

The “Overarching Information Sharing Agreement for Direct Care” lists the legal gateways for information sharing in support of health and social care integration – (see below). However, the legal gateways listed refer specifically to adult social care. Most guidance, including that from the National Data Guardian suggests that children’s information should be dealt with in a similar manner.

The following legislation supports information sharing for direct care:

- The Health and Social Care (Safety and Quality) Act 2015
- The Health and Social Care Act 2012
- The Personal Care at Home Act 2010
- Safeguarding Vulnerable Groups Act 2006
- National Health Service Acts 1977 & 2006
- Mental Capacity Act 2005
- Children Act 1998 & 2004
- Local Authority Social Services Act 1970 as amended by the Health & Social Care (Community Health & Standards) Act 2003
- NHS Bodies and Local Authorities Partnership Arrangements Regulations 2000
- Local Government Acts 1972 & 2000
- Data Protection Act 1998
- Human Rights Act 1998
- Access to Health Records Act 1990
- National Health Service and Community Care Act 1990
- Chronically Sick and Disabled Persons Act 1970
- National Assistance Act 1948

Section 3 of the Health and Social Care (Safety and Quality) Act 2015 requires relevant health or adult social care commissioners or providers to disclose information to other health or adult social care commissioners to facilitate the provision of health services or adult social care in the best interest of the patient / service user. The duty of confidence must still be considered.

For this information sharing agreement the following legislation is relevant in addition to that quoted in the "overarching agreement":

"The Children Act 2004, Section 10: Co-operation to improve well-being."

The National Health Service Act 2006, Part 3 Section 82 – Co-operation between NHS bodies and local authorities

The Health and Social Care (Safety and Quality) Act 2015, 3 Duty to share information

The Article 6 basis is processing "is necessary for the performance of a public task carried out in the public interest".

See also:
School Immunisation Programme
https://www.nice.org.uk/guidance/ph21/chapter/1-Recommendations#recommendation-2-information-systems

Local Authorities

The Localism Act 2011

The Localism Act 2011 provides a power of general competence for local authorities. Part 1, chapter 1, section 1 states, subject to prescribed limitations including compliance with pre-existing legislation:

"(1) A local authority has power to do anything that individuals generally may do.

(4)(c) for the benefit of the authority, its area or persons resident or present in its area."

The local authority is empowered to share information, if it believes that there is reasonable justification to do so for the benefits of the area, residents and communities. The sharing of information proposed is justified because it assists practitioners to design and deliver timely interventions for individuals and families. This provides benefits to those individuals and families, by improving the services that they receive and benefits the wider community by using public resources in the most efficient and effective way possible.

Local Government Act 2000

The Act gives local authorities powers to take steps which they consider are likely to promote the wellbeing of inhabitants in their area.

The main power specific to local authorities is section 2 – the power of "well-being". This enables local authorities to do "anything" to promote social, economic, or environmental well-being in their area provided the act is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out the act it gives regard to its own community strategy. Section 111 Local Government Act enables local authorities to anything conducive or incidental to the discharge of its functions, providing it has specific statutory authority to carry out those main functions in the first place. Section 2(4) makes clear that the power in section 2(1) enables authorities to work in partnership with

other bodies. For example, it allows authorities to assist other statutory bodies to discharge their functions, or to exercise those functions on their behalf e.g.

(1) This section applies where a local authority has reasonable cause to suspect that an adult in its area (whether or not ordinarily resident there):-

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

(2) The local authority must make (or cause to be made) whatever enquiries it thinks necessary to enable it to decide whether any action should be taken in the adult's case (whether under this Part or otherwise) and, if so, what and by whom.

(3) "Abuse" includes financial abuse; and for that purpose "financial abuse" includes:-

(a) having money or other property stolen,
(b) being defrauded,
(c) being put under pressure in relation to money or other property, and
(d) having money or other property misused

NHS Bodies

Section 82 of the National Health Service Act 2006 sets out a duty to co-operate between NHS bodies and Local Authorities in order to secure and advance the health and welfare of the people of England and Wales.

The Health Act 1999, Section 27 states that NHS bodies and local authorities shall co-operate with one another in order to secure the health and welfare of people.

Common Law

The duty of confidentiality has been defined by a series of legal judgements and is a common law concept rather than a duty contained in statute. Where information is held in confidence, such as personal information about patients held by medical practitioners, the consent of the individual concerned should normally be sought prior to any information being disclosed. Common law judgements have, though, identified a number of exceptions and have determined that information held in confidence can in certain circumstance still be disclosed without the individual's consent. Where they can be demonstrated, factors that may justify disclosure include:

- It needs to be shared by law
- It is needed to prevent, detect and prosecute serious crime
- There is a public interest
- There is a risk of death of serious harm
- There is a public health interest
- It is in the interest of the person's health
- It is in the interests of the person concerned

Specific measures to prevent crime, reduce the fear of crime, detect crime, protect vulnerable persons, maintain public safety or prevent offenders from reoffending are in the public interest. However, there still needs to be a careful balancing exercise in each case to ensure that the disclosure (including the extent of the disclosure) is justified on the basis of an overriding interest.

(National Support Framework, Delivering Safer and Confident Communities: Information sharing for community safety: Guidance and practical office, Home Office)

The Children's Act 2004

Section 10 of the Children Act 2004 places a duty on Children's Services Authorities to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area and for the police and other local authorities to co-operate in those arrangements. This includes:

- Physical and mental health, and emotional well being
- Protection from harm and neglect
- Education, training and recreation
- Making a positive contribution to society
- Social and economic well-being

Section 11 of the Children Act 2004 places a duty on local authorities and the police to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children.

The Children's Act 1989

Local authorities have a duty to safeguard and promote the welfare of children within their area who are in need. Local Authorities may collect and share information under these implied powers in order to support/protect children.

Sections 17 and 47 place a duty on local authorities to provide services for children in need and through.

Section 27 to elicit the co-operation of key partner agencies (including other local authorities, education authorities, housing authorities, PCT's and NHS Trusts) to assist them.

Section 47 places the same agencies under a similar duty to assist local authorities in carrying out enquiries into whether or not a child is at risk of significant harm.

Section 17 enable the local authority to request help from other local authorities, and NHS bodies and places an obligation on these authorities to cooperate. Part 1 Schedule 2 Para. 1 requires local authorities and professionals in other sectors to take reasonable steps to identify children in need. Para. 4 to prevent children from suffering ill treatment or neglect.

Appendix B: DPA and GDPR compliance

Human Rights Act 1998

HUMAN RIGHTS ACT 1998 Article 1 - the right to life. Article 3, no one should be subjected to torture, inhuman or degrading treatment and Article 8 of the European Convention on Human Rights gives individuals the right to respect for private and family life, home and correspondence. This right cannot be interfered with by a public authority unless this is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.	The purposes for which the information is being shared under this ISA is: • the protection of health or morals,
Proportionality	Partners will ensure that information requested or shared under the terms of this agreement is relevant, necessary and proportionate

General Data Protection Regulation and Data Protection Act 2018

The legal basis that underpins this relationship and the requisite duties and powers to facilitate the lawful sharing of appropriate information between partners is taken from Principles I - 6 of the GDPR plus rights of individuals and data transfer outside of the EU. Where all these requirements are satisfied, the sharing of information will be lawful. Therefore, the requirements of each principle and requirement together with how the partners to this arrangement will meet them are summarised below.

First Principle

First Principle Requirements of Lawfully and Fairly	**How will partners satisfy these requirements?**
ULTRA VIRES RULE The ultra vires rule and the rule relating to the excess of delegated powers under which the data controller may only act within the	The partners are relying upon the legislation in Appendix A to provide the vires to share information with the partners to this agreement.

limits of its legal powers.	
LEGITIMATE EXPECTATION Legitimate expectation, that is, the expectation of the individual as to how the data controller will use the information relating to him.	It is argued that where an individual is the subject of any of the sharing activities listed in this agreement, that individual must reasonably expect that agencies involved with supporting the law enforcement function or other relevant functions will share information required to effectively undertake those functions. Partners will proactively communicate to individuals and the community at large that this sharing takes place.
FAIR PROCESSING & TRANSPARENCY When data are obtained from data subjects the data controller must ensure, so far as practicable that the data subjects have, are provided with, or have made readily available to them, the following information:- (a) the identity of the data controller (b) if the data controller has nominated a representative for the purposes of the Act, the identity of that representative (c) the purpose or purposes for which the data are intended to be processed (d) any further information which is necessary taking into account the Specific circumstances in which the data are or are to be processed to enable processing in respect of the data subject to be fair.	Fair processing information as described in GDPR Articles 12(1), 12(5), 12(7), 13, 14 and / or DPA18 Section 44 (1) shall be provided by the involved data controllers to data subjects. Partners will proactively communicate to individuals and the community at large that this sharing takes place. This will be achieved through publication of Privacy Notices on agencies external web-sites, press releases, social media publications and other local communication options appropriate to each agency.
First Principle Requirements to satisfy conditions in ARTICLE 6 of GDPR	**Please see the table below**
First Principle Requirements to satisfy conditions in ARTICLE 9 of GDPR (and derogations by member states in the DPA18)	**Please see the table below**

Data	**GDPR**	**DPA 18**
Personal Data	6(1)(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise	Data Protection Act 2018, Part 3 Section 35 (2) (b) – ***'Public Duty'.*** (please see Appendix A for further details on partners statutory obligations)

	of official authority vested in the controller; DPA18 Section 8 Lawfulness of processing: public interest etc.	Statutory etc or government purposes. **DPA 2018 Schedule Conditions met**: Schedule 1, Part 1, 2 - Health or social care purposes Schedule 1, Part 1, 3 – Public health purpose

s.

Second Principle

Second Principle Requirements	**How will partners satisfy these requirements?**
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;	Sections 1, 4.1.1 and 5 details the Purpose the information can be processed for and the constraints/limitations on further processing.

Third Principle

Third Principle Requirements	**How will partners satisfy these requirements?**
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	The minimum amount of personal data is being shared to achieve the purpose.

Fourth Principle

Fourth Principle Requirements	**How will partners satisfy these requirements?**
Personal data shall be accurate and, where necessary, kept up to date	Partners will not take any operational action in relation to an individual about whom information has been exchanged without first checking with the source of the data to ensure it is still current. e.g. Note the comments below about the 5th principle. Ensure users update records, correct

	incorrect information and close cases in accordance with operating procedures and identify those records where the accuracy of the information is uncertain.

Fifth Principle

Fifth Principle Requirements	How will partners satisfy these requirements?
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	Retention and disposal policies of partner organisations will be adhered to.

Sixth Principle

Sixth Principle Requirements	How will partners satisfy these requirements?
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	Partners to this agreement will apply the security necessary to comply with Appendix B. Police information stored on partners' systems will only be available to staff who need that information to carry out the purpose.

Data Subject Rights

Data Subject Rights Requirements	How will partners satisfy these requirements?
Personal data shall be processed in accordance with the rights of data subjects under this Act.	Partners to this agreement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed. In the event that a subject access request is received by a partner and personal data provided by another partner is identified, the partners will liaise and assess whether an exemption is appropriate.

Transfer Outside of the EU

Transfer outside of the EU	How will partners satisfy these requirements?
Transfers must be subject to appropriate safeguards	Wherever possible data will be stored and transferred only in the UK or EU. If transfer takes place it must be to a country with an Adequacy decision or using EU contract clauses or equivalent.

Appendix C

Data to be shared

From Partner Organisation	To Partner organisation	System (if relevant)	Data to be Shared
RCC	LPT	n/a	Child name, parent name and contact details
LPT			

Appendix D

Service Contact Details

Name of Responsible Officer	Partner Organisation	Tel. No.	Email address
Bernadette Caffrey	RCC	01572 720943	bcaffrey@rutland.gov.uk
Rosie Jones	LPT	0116 295 1361	rosie.jones@leicspart.nhs.uk

Appendix E

Information Security Standards

1. Each Partner agrees to hold all information shared under this agreement in accordance with security standard ISO 27001 or an equivalent level of compatible security.

2. Each Partner accepts it is for each Partner to assess its security needs and identify what is and is not needed by it in order to comply with this agreement and its obligation as a data controller.

3. Where a Partner has specific security needs to comply with a specific standard or requirement, for example Caldicott, it should specify these and they will be included in this Appendix. This can be either as a .pdf document or by means of a hypertext link to the specifying Partner's site. It is then for the other Partners to ensure that they take these standards into consideration when assessing their own security needs.

4. Where a Partner has specified its security needs it is for that Partner:
   i) to provide to the other Partners updates of its security needs from time to time to keep those Partners and this document up to date. These should be provided to the other Partners at least three months before such changes are due to be effective; and
   ii) to confirm as part of its review process that nothing has changed to the reviewing body.

5. Each Partner shall ensure that:
   - unauthorised staff and other individuals are prevented from gaining access to personal and sensitive personal data shared under this agreement;
   - visitors to its premises are received and supervised at all times in areas where personal data and sensitive personal data shared under this agreement is stored;
   - all computer systems that contain personal data and sensitive personal data shared under this agreement are password-protected;
   - only those who need to use the data shared under this agreement for the Purpose have access to it;
   - all new software is virus-checked prior to loading onto the Partner's information technology system or onto any removable storage device upon which the Partner has stored personal data shared under this agreement.

6. Each Partner shall ensure that its officers, staff, authorised contractors and authorised representatives:
   - do not leave their workstation/PC signed on when it is not in use;
   - minimise access to information and do not allow others to view the information displayed on their screens or in printouts that they are not entitled to view;

- lock away disks, tapes or printouts when not in use;
- exercise caution in what is sent via email and to whom it is sent. Emails containing personal information should be sent by secure email or if it has to be sent by insecure email the personal information must be contained within a password protected attachment and not set out in the body or header of the email;
- check that the intended recipient of a fax containing personal data is aware that it is being sent and can ensure security and confidentiality on receipt along with confirming receipt;
- ensure that their paper files are stored in secure locations and only accessed by those who need and are authorised to use them;
- do not disclose personal data to anyone other than the data subject unless they have the data subject's consent, or it is a registered disclosure, required by law, or permitted by a relevant and lawful exemption to the Act ;
- do not leave personal, sensitive personal or sensitive project operational information on public display in any form;
- adhere to a clear desk policy and, in particular, ensure that at the end of each day sensitive material is locked away securely.

7. Each Partner agrees that any information disclosed or shared in accordance with this agreement which relates to identifiable individuals shall be classified as "Official- Sensitive'" and each Partner shall ensure that its officers, staff, authorised contractors and authorised representatives handle that information as instructed below or in accordance with their own information handling scheme.

	OFFICIAL including OFFICIAL-SENSTIVE
Physical Security a. Document handling	○ No requirement to mark documents with **OFFICIAL** marking ○ Comply with the Clear Desk – Clear Screen policy ○ **OFFICIAL-SENSITIVE** the document must be marked at the top and bottom of each page and handling instructions considered, e.g. ○ FOR AUTHORISED PERSONNEL ONLY ○ TO BE OPENED BY ADDRESSEE ONLY ○ NOT FOR FORWARD DISSEMINATION ○ NO PHOTOCOPYING WITHOUT PERMISSION OF ***AUTHOR***
b. Storage	○ **OFFICIAL** - Storage behind a single locked barrier. **OFFICIAL – SENSTIVE** – consider a second locked barrier. ○ **OFFICIAL-SENSITIVE** - Consider use of approved physical security equipment/furniture
c. Remote Working	○ Ensure information cannot be inadvertently overlooked whilst being accessed remotely ○ Store assets under lock and key at remote locations
d. Moving assets by hand	○ Single cover with no external markings – sealed transit envelope is acceptable ○ **OFFICIAL-SENSITIVE** – Sealed envelope – no external

	OFFICIAL including OFFICIAL-SENSTIVE
	markings ○ Precautions against overlooking when working in transit (e.g. whilst travelling by train)
e. Moving assets by post/courier	○ Sealed envelope, never mark classification on envelope ○ **OFFICIAL-SENSITIVE** - Consider double enveloping ○ If sending sensitive personal data externally use registered Royal Mail service or reputable commercial courier's 'track and trace' service
INFORMATION SECURITY a. Electronic Information at Rest	○ Electronic data at rest can be found on computers, mobile devices etc. This information is protected according to its sensitivity; for portable devices data will be encrypted. ○ Appropriate controls to protect the information may be physical protection, such as a locked door or may involve encrypting data that would be classified as **OFFICIAL-SENSITIVE**
b. Electronic Information in Transit e.g. e-mail	○ Remember, ALL emails are at least **OFFICIAL** ○ Information between Police forces, government and trusted organisations is via secure networks, e.g. '.pnn' e-mail ○ If the email does not contain sensitive information you can send it over the insecure internet e.g. anyone@anywhere.com ○ Do not send sensitive information to insecure internet domain addresses, such as Google mail, Hotmail, Yahoo, consider redacting the information if appropriate ○ Where more sensitive information must be shared with external partners or members of the public, consider using secure mechanisms such as password protected documents. Consider file encryption for **OFFICIAL-SENSITIVE** together with handling instructions. ○ Where more sensitive information must be shared with external partners, ensure secure mechanisms (e.g. browser sessions using SSL/TLS) are used. ○ You should provide handling instructions if necessary, based on your risk assessment and at **OFFICIAL-SENSITIVE** ○ In **exceptional** circumstances, where there is a requirement for information to be sent unencrypted over the Internet, you have to make a risk-balanced decision; there is always a risk of information being intercepted and exposed. It is very important to stipulate handling instructions in this scenario.
c. Removable Media (data bearing)	○ All portable and removable media must be encrypted and only Force supplied devices are to be used ○ Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement
d. Telephony (mobile and landline), Radio, Video Conference and Fax	○ Details of sensitive material should be kept to a minimum – be aware of being overheard and your surroundings ○ Your conversation, video conference etc. may be recorded by the other or a third party ○ Faxing is only acceptable as a last resort, where the recipient

	OFFICIAL including OFFICIAL-SENSTIVE
	does not have a secure e-mail and there isn't time to send via post ○ Recipients should be waiting to receive faxes containing personal data and/or data marked with the **OFFICIAL – SENSITIVE** caveat
Destruction of Hard Drives etc.	○ All disposal of IT equipment must be carried out by the Information Services Department
Disposal / Destruction of paper	○ Destroy using equipment which meets a recognised international paper destruction standard, designed to consistently destroy to particles no larger than 4 x 15 mm
Incident Reporting	○ Follow incident reporting procedures set out in the relevant Security Policy