Operation Encompass

INFORMATION SHARING AGREEMENT

PURPOSE	To facilitate the sharing of police material pertaining to domestic violence to schools, academies and colleges to enable early intervention and support to affected children and young persons.

Partners
Leicestershire Police Leicester City Council Leicestershire County Council Rutland County Council

Date agreement comes into force:	When signed

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

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

Agreement Drawn up by:	Catherine Smith, Leicestershire Police

Protective Marking:	OFFICIAL

Reference Number:	ISA 2025: Op Encompass

VERSION RECORD

Version No.	Amendments Made	Authorisation	Date
1.0	Initial draft	[Catherine Smith, Leicestershire Police]	November 2025
1.1	Minor amendments by Force DPO	Steven Morris, Leicestershire Police	December 2025
1.2	Additional personnel details	*Catherine Smith, Leicestershire Police*	*December 2025*

1. Policy Statements and Purpose of this Information Sharing Agreement

1.1 Purpose and Justification for Information Sharing

This Information Sharing Agreement (ISA) has been developed between the Chief Constable of Leicestershire Police and the Local Authorities of Leicester, Leicestershire and Rutland, in order to govern schools, academies and colleges and any other educational settings including (but not limited to) alternative provision, the Virtual School, Inclusion Services and Educational Welfare, under Operation Encompass.

Operation Encompass is a multi-agency approach enshrined in law, to give early notification to schools, academies and colleges that domestic abuse has happened within a child's immediate family, or within their home, or has witnessed domestic abuse. Designated Safeguarding Leads within schools will receive information from Leicestershire Police to afford them the opportunity of providing silent support to the child through a variety of methods to be decided upon by schools, not limited to greeting the child at the beginning of the day, providing a platform for any disclosure, and providing classroom support. In order for the setting to be able to adequately support the child, the DSL must be Operation Encompass trained.

Partners have agreed to share information in line with the updated laws around Operation Encompass, and in order to formalise and properly govern the information sharing. By Leicestershire Police sharing the information directly with educational settings, we will maintain control over the information, and strengthen our relationships with education.

The ISA contains a signatory section through which partners acknowledge and accept the requirements placed upon them and others within their organisations by the ISA.

The partners agree that for the purposes of this ISA the term 'sharing' information means providing or disclosing information including personal data to another partner by any means and/or the receiving or collection information including personal data from another partner by any means.

In some instances, partners may all share information with one another; in some cases, a partner may share info with another partner(s), but not receive shared information from partners.

In the instance where a setting has received information regarding a child who is not on role with them, the setting will immediately inform Leicestershire Police by emailing:

CAIUREFERRALS@LEICS.POLICE.UK. The setting will not forward the information to another setting, other than an alternative provision which is under the authority of the setting.

The partners agree that the specific, explicit and specific purpose(s) for sharing information are to provide school safeguarding leads with information relating to children who are pupils at their school that have experienced a domestic abuse incident. Leicestershire Police will complete this referral upon attendance at the incident, therefore usually prior to the child's subsequent day at school. This referral will enable

the ‘Designated Safeguarding Lead or Key Adult’ to provide appropriate care and welfare to the child whilst they are at school.

Police officers attending incidents of domestic abuse irrespective of the grading or risk will provide the name of a child to the school’s dedicated safeguarding Key Adult practitioner via secure and encrypted email in cases where a child between the ages of 4 to 17 is either present at the domestic abuse incident, ordinarily resides at the address, or ordinarily resides with an adult involved in the incident as a victim or suspect.

This will be transferred on a single referral form under the cover of an **‘Operation Encompass Referral’**. The provision of this information will enable **Key Adults specifically trained** in Operation Encompass to have earlier and more informed information to plan and provide an intervention with the child to reduce the impact of the trauma.

Knowing about a domestic abuse incident through Operation Encompass (especially when it is done prior to the child’s next attendance to school) will enable the Key Adult to keep a close eye on their emotional state, understand why the child may be presenting in a certain manner and make adjustments and proactively offer support. This will also reduce the risk of a multiple effect (an effect caused by the DA incident) that might occur if the child exhibits an anger reaction to events.

2. Governance

This Agreement sits under the over-arching Leicester, Leicestershire & Rutland (LLR) Information Sharing Protocol (ISP), 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.)

As required by GDPR and/or the Data Protection Act 2018, a Data Protection Impact Assessment has been carried out on information sharing activity within this ISA.

This ISA demonstrates compliance with the accountability principle under GDPR Article 5(2) and Section 34(3) DPA 2018.

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. 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. 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 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.

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.

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

The partners agree that any information shared under the processes described in this ISA will only be used or handled in accordance with the terms set out in this ISA.

The partners agree not disclose the personal information obtained under this ISA to other parties or organisations not party to this ISA except where required to do so by law.

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

The data will be shared only with the nominated trained safeguarding lead ('Key Adult') for that particular child's school. It will be used for the single purpose of providing school Key Adult safeguarding leads with information to assess the appropriate provision of welfare and pastoral support to the child at their school. The data is recorded on a single referral form which is stored on Police systems and by safeguarding leads on existing school's databases relevant to the secure school record for the child.

The personal data will be shared by way of secure email directly to the DSL. 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 and a Partner uses the information to the extent 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

9 How long will it be retained by the parties?

Partners accept that they must only store shared information in a form that identifies individuals for as long as is necessary for the purposes for which they processing the personal data.

The partners also agree that they must each have and implement comprehensive retention schedules, which:

- Set out the minimum necessary period of storage for different categories of personal data, which are determined taking into account:
    - The types of personal information that processed (organised, for example, by function);
    - The purposes for processing the personal information;
    - Why each type of personal information should be retained
    - Any relevant industry standards or guidance;
    - Any relevant legal obligations to retain personal data for specific periods of time.
- Set out where the personal information will be stored and how it will be kept secure during the retention periods.
- Set out how any processors who process information on their behalf will comply with their retention periods.
- Set out how data will be archived or destroyed.

The partners agree to have systems in place to adhere to the periods in their Retention Schedules and to review their Retention Schedules regularly. They will train their staff so that they are empowered to comply with our Retention Schedules.

The partners agree that where a partner is disbanded the partner will ensure that the shared personal data held by it is disposed of securely and confidentially. Alternatively, where the partner is replaced by a successor organisation, it will ensure that the personal data held by it is properly transferred to its successor organisation, subject to the successor organisation becoming a signatory to this ISA. If the successor does not wish to become a signatory to this ISA, the personal information will be disposed of securely and confidentially.

10 Security and Vetting

The partners agree to put in place appropriate physical, technical and organisational measures to protect any information provided to them under this ISA.

The partners accept the requirement to ensure that any employees are able to access only the shared personal data necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to personal data and Data Protection legislation.

The partners agree to maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.

The partners agree to protect the physical security of the shared information. This means they will, as a minimum:

- Ensure their organisation controls physical access to its premises;
- Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises;
- Ensure proper physical control of printers and photocopiers so that personal information is not left lying on the printer/photocopier;
- Ensure secure disposal of printed materials, so that materials intended for disposal do not sit around in piles. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises;
- Ensure that old computers, printers and other electronic equipment is disposed of safely and that all personal information is irretrievably scrubbed from any memory before disposal.

The partners agree to protect the electronic security of the shared information. This means they will, as a minimum:

- Ensure their organisation has a strong password policy that is adhered to by all staff members. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members;
- Ensure their organisation installs security patches on electronic devices (including ensuring all operating systems' updates are installed in line with best practice);
- Ensure staff are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work;
- Ensure that any information that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice;

The partners agree to ensure that all shared information held on portable devices, including laptops, tablets and USB/portable drives is kept secure in line with national best practice and regulatory guidelines.

The partners agree to have contracts and systems in place to ensure that any contractors and subcontractors managing any aspect of information security are fully aware of and abide by this ISA.

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.

14 Review of Information Sharing Agreements

This Agreement will initially be reviewed 12 months after signature and then 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.

15 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 must be 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.

16 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.

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

Subject Access Requests and other notices relating to a data subjects rights made under the GDPR and DPA18 will be co-ordinated and responded to by the organisation receiving 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 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 GDPR and DPA18 as they see fit.

18 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.

19 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	**Chief Officer or Senior Information Risk Owner (SIRO)**	**Date**	**Signature (CO/SIRO)**	**Information Security Contact Name &Number**
Leicestershire County Council		05.01.2026		Sharon Cooke
Leicestershire Police	DCC Michaela Kerr	20/02/2026		Steven Morris – DPO@leics.police.uk
Leicester City Council	SIRO	09/02/2026		Alison Greenhill 0116 454 4001
Rutland County Council	Angela Wakefield	10/02/2026	DocuSigned by: Angela Wakefield ED0944FE70594C1...	Katherine Jamieson- dataprotection@rutland.gov.uk 01572758304
Huncote Primary School	Sally Houghton (Headteacher)	23/02/2026		office@huncote.embracemat.org 0116 286 4105

Appendix A: Operation Encompass **– Legislative Framework**

The partners agree that the lawful basis for sharing are that this is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority (Article 6(e) GDPR). The processing is strictly necessary and applies to **safeguarding children and individuals at risk** and is in the substantial public interest for the purpose of safeguarding children (DPA 2018, Sch.1, Part 2, S.18).

The Victims and Prisoners Act (2024)

The Victims and Prisoners Act 2024 defines victims as those who have "suffered harm as a direct result of" being subjected to, directly experiencing, born as a result of, bereaved of a close family member as a result of, and of being a child victim of criminal conduct. The Act goes on to specify amendments to the Domestic Abuse Act (2021) namely:

> A chief officer of a police force must ensure that arrangements are in place to notify relevant educational establishment as soon as is reasonably practicable. (S49A)

Working Together to Safeguard Children (2023)

The updated guidance document emphasizes a push towards working more closely with schools, and information sharing. There are a number of requirements which fall within the Operation Encompass umbrella:

> *29. Practitioners should be proactive in sharing information as early as possible to help identify, assess, and respond to risks or concerns about the safety and welfare of children.*
>
> *77. LSPs should create an environment which enables all schools… early years… and childcare providers in the local area to be fully engaged, involved and included in local safeguarding arrangements.*
>
> *88. Safeguarding partners should have an agreement in place which outlines how information is shared safely and effectively between themselves and other relevant agencies.*
>
> *128. Safeguarding professionals, including safeguarding partners and their delegates, should work closely with education and childcare settings to ensure information about children is shared effectively*

The Childrens Act (2004)

> Details the duty to promote co-operation between agencies with a view to improving the well-being of children in the local area (S10)

And the duty to ensure that the agency's functions are discharged having regard to the need to safeguard and promote the welfare of children (S11)

The Police Act 1996

The Police Act 1996 gives police constables certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and assisting the public. This allows the disclosure of identifiable information on a case-by-case basis for these purposes subject to appropriate safeguards.

The police also have a general common law power to disclose information for policing purposes[1].

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; or
- 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)

[1] The Policing Purpose – which includes the prevention and detection of crime; apprehension and prosecution of offenders; protecting life and property; preserving order; maintenance of law and order; rendering assistance to the public in accordance with force policies and procedures; and any duty or responsibility of the police arising from common or statute law.

In short, we are required by law to share information with schools, to be proactive in our information sharing and our engagement with schools, to have an agreement in place which outlines safe sharing of information, and to work closely with education and **childcare settings**. Legally, the requirement is to share with schools and childcare settings. This Information Sharing Agreement only governs sharing of information with schools, academies, colleges and educational settings including alternative provision, Inclusion Services and Educational Welfare.

The sharing of Data through Operation Encompass is required to achieve the aim of providing information for schools to assess the appropriate levels of care to the child within the school environment. This cannot be achieved by other means as schools do not routinely have access to information relating to police attendance at domestic abuse incidents where their pupil may have been (present and or) experiencing

The use of personal data is proportionate to the aim of the proposal. The advantages of sharing data with schools relating to children exposed to domestic abuse incidents can have a profound impact on individuals' lives, particularly in considering children and their continued and sustained exposure to adverse childhood experiences (ACEs). The advantages to sharing this data with schools could ensure that an individual receives the right services at the right time and may also prevent the needs of a child from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death.

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: • To protect life • To prevent torture, inhuman or degrading treatment • To support public safety, • the protection of health or morals, • the prevention of disorder or crime and • to protect the rights and freedoms of others.
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	The partners are relying upon the legislation in Appendix A to provide the vires to share information with the

powers under which the data controller may only act within the limits of its legal powers.	partners to this agreement.
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)(c) processing is necessary for compliance with a **legal obligation** to	Data Protection Act 2018, Part 3 Section 35 (2) (b) – ***'Public Duty'.*** (please see Appendix A for further

	which the controller is subject; (please see section Appendix A for further details on partners statutory obligations); 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; 6(1)(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party; DPA18 Section 8 Lawfulness of processing: public interest etc.	details on partners statutory obligations)
Special Category Data (sensitive processing of personal data DPA 18)	Article 9 processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	DPA Part 3, Chapter 2 S35 (5) (a) & (b) – the processing is ***strictly necessary*** for law enforcement purposes and condition in schedule 8 must be met. Schedule 8 – DPA 2018 condition that is met under this Agreement Paragraph 1 – *Statutory purposes* (a) is ***necessary*** for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is ***necessary*** for reasons of substantial public interest

		Additional conditions met in accordance with s10(3) DPA DPA Schedule 1 Part 2; *Para 6 - Statutory etc and government purposes* 6 (1) This condition is met if the processing— (a) is necessary for a purpose listed in sub-paragraph (2), and (b) is necessary for reasons of substantial public interest. (2) Those purposes are— (a) the exercise of a function conferred on a person by an enactment or rule of law; (b) the exercise of a function of the Crown, a Minister of the Crown or a government department.
Criminal Offence Data		DPA 2018, Part 2, chapter 2; s.10(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority. s.10(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1. Additional conditions met under DPA, Schedule 1, Part 2 *Para 6 - Statutory etc and government purposes*

		6 (1) This condition is met if the processing— (a) is necessary for a purpose listed in sub-paragraph (2), and (b) is necessary for reasons of substantial public interest. (2) Those purposes are— (a) the exercise of a function conferred on a person by an enactment or rule of law; (b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

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
Educational settings	Leicestershire Police	Email	PPN email in the event that the child is not on their role

Appendix D

Service Contact Details

Name of Responsible Officer	Partner Organisation	Tel. No.	Email address
	Leicester City Council		
	Leicestershire County Council		
	Rutland County Council		

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; and
   - 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.