Supporting Leicestershire Families/Think Family/Changing Lives

INFORMATION SHARING AGREEMENT

PURPOSE	The purpose of this document is to facilitate the lawful and safe exchange, use and security of personal data and sensitive personal data, in order to ensure that the business objectives of the Supporting Leicestershire Families/Think Family and Changing Lives Programme are met.

Partners for Supporting Families programme	
Leicestershire County Council	
Leicester City Council	
Leicestershire Police	
Leicester City Youth Offending Service	
Leicestershire Youth Offending Service	
Probation	
NHS Leicestershire Partnership Trust	
DWP	
Rutland District Council	
Blaby District Council	
Charnwood Borough Council	
Harborough District Council	
Hinckley and Bosworth Borough Council	
Melton Borough Council	
North West Leicestershire District Council	
Oadby and Wigston District Council	
Working Links (City Council ESF Provider)	
Women's Aid Leicester Ltd (County Domestic Violence Service)	

Date agreement comes into force:	October 2013

Date of Agreement Review:	October 2014 then 5 yearly thereafter

Agreement Owner:	Strategic Information Management Group

Agreement Drawn up by:	Anne Chafer, Lynn Wyeth, Gill Wood

Protective Marking:	Not Protectively Marked

VERSION RECORD

Version No.	Amendments Made	Authorisation	Date
V3	Draft submitted to CC and CBC	Anne Chafer	17/02/2013
V4	Amendments made by SLF Partners		25/02/2013

V5	Minor amendments		06/03/2013
V6	Amendments to Appendices	Jeff Hardy	13/03/2013
V7	Minor service amendments	Gemma Whysall	15/03/2013
V8	Minor amendments	Anne Chafer	22/04/2013
V9	Add Leicester City Council and Rutland DC into ISA	Anne Chafer	03/07/2013 26/07/2013
V10	Add comments from City and County Add security appendix	Anne Chafer	10 – 11/09/2013
V12	Add legal basis for NHS, Probation and YOS and amend table per CC response from Sam Kirkland. Add re deletion of information after data matching - para 4.3.1 and s10	Anne Chafer	17/09/2013 14/10/2013

1 State the specific purpose of this information sharing

The purpose of this information sharing is to ensure:-

- The effective identification of families for Payment by Results (PbR) and assessment for inclusion on the Supporting Leicestershire Families (SLF) /THINK Families (TF)/Changing Lives Programme (hereinafter referred to as the Programme).
- The effective provision of support and challenge interventions, provided by Key Family Support Workers and members of designated Teams around the Family (TAF).
- Improved outcomes for the families.
- Reduction over time of demand on the partners from these families.
- The effective measurement of progress made by families whilst being supported.
- The effective measurement of outcomes, to support payment by results claims and nationally and locally agreed indicators.
- The effective evaluation of the programme.
- The minimum amount of personal and sensitive personal information which is necessary to achieve the purpose in order to reduce the privacy impact upon the families and the resource implications upon the partners.

2 Governance

This agreement has been drawn up with reference to the Leicestershire Information Sharing Protocol which has been signed by the partners listed above.

3 Legal Basis for Information Sharing

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 the Data Protection Act 1998 and/or the Human Rights Act 1998 and is necessary for compliance with principle 1 of the Data Protection Act. Section 3.4 identifies statutory gateways for information exchange that apply to the partner agencies for the purpose of this agreement.

3.1 Data Protection Act 1998

In addition, disclosure must be compliant with the Data Protection Act 1998 and the ways in which this information sharing will comply with the principles is set out in **Appendix A**. 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.

Where there is a need to share personal and sensitive personal information[1] each partner must be able to identify a condition in Schedule 2. If sensitive personal data are being shared, a Schedule 3 condition must also be identified before the information can be processed and shared. The Schedule 2 and 3 conditions for each partner are set out in **Appendix A**.

3.2 Human Rights Act 1998 (HRA)

The Human Rights Act applies to all public authorities and parties to this agreement endeavour to ensure that the principles of the Human Rights Act 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 or 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 and sensitive personal data to be shared to implement this Programme has been identified as that necessary to enable the effective identification of families in order to facilitate on going support and challenge interventions to those families and individual members in order to prevent further crime or disorder and the protection of the rights and freedoms of others. The

[1] Both personal data and sensitive personal data are defined in the Information Sharing Protocol.

collection of outcome data for both performance management and payment by results is necessary to fund this Programme. The partners will share the minimum amount of personal data and sensitive personal data necessary to achieve the purpose identified in Section 1 and this is proportionate to the purpose and justifies the interference with the Article 8 rights of the data subjects.

3.3 Equality

Equality issues are being considered with regard to the Programme. This will ensure compliance with Equality and Diversity legislation and internal Equality and Diversity policies.

3.4 Statutory Gateways Relevant to the Sharing of Information for this Programme.

3.4.1 Police

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 when ever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.
The police also have a general common law power to disclose information for policing purposes.

3.4.2 Local Authorities, Police, Probation and Health

Section 115 (a) and (b) of the Crime and Disorder Act 1998 confers a power on any person to disclose information to a relevant authority (which are the police, local authority, health authority and probation service or to any other person acting on behalf of such authority) which is necessary or expedient to help implement the provisions of the Act, which include contributing to local strategies to reduce crime and disorder, seeking anti-social behaviour orders and consultation prior to seeking such orders.

S17 of the Crime & Disorder Act 1998 - All partners to this agreement are under a legal obligation imposed by Section 17 Crime and Disorder Act 1998. This imposes a duty upon the Police, local authorities, health and probation to exercise their functions with regard to the effect on and to do all that they reasonably can to prevent crime and disorder in their area.

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.

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.

This is further supplemented by Section 1E of the Crime and Disorder Act 1998 (as amended by section 66 of the Police Reform Act 2002). This requires consultation

between relevant agencies to share Information in support of ant-social behaviour order applications.

3.4.3 Local Authorities

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.

Section 111 of the Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions

S17 Children 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.

3.4.4 Department of Work and Pensions

Welfare Reform Act 2012 – Section 134 allows for longer term data sharing powers between DWP, their service providers and local authorities in particular to Troubled Families and their in work and out of work benefits

3.4.5 NHS Trust

Part III, Section 27 Children Act 1989 – stipulates that there is a duty to cooperate between authorities:

'(1)Where it appears to a local authority that any authority mentioned in subsection (3) could, by taking any specified action, help in the exercise of any of their functions under this Part, they may request the help of that other authority specifying the action in question.

(2)An authority whose help is so requested shall comply with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions.

Section 31 of the Health Act 1999 – makes provision for NHS and Local Authority bodies to engage in activities that are health related if it demonstrates improvement

in the way that the functions are delivered. This includes the provision of individual services to individuals

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 NHS and other local authorities to co-operate in those arrangements.

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.

3.4.6 Youth Offending Service (YOS)

YOS have a statutory duty to coordinate the provision of youth justice services including advising courts, supervising community interventions and sentences, and working with secure establishments in respect of young people serving custodial sentences and also in the latter category of a children's service.

As YOS are multi-agency teams, members will also need to be aware of the need to safeguard and promote the welfare of children that relates to their constituent agency.

4 Information - What information is it necessary to share?

4.1 Personal Data

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 data controller. Additional guidance is given in the Information Sharing Protocol. Section 3.4 above sets out the statutory gateways under which personal data may be exchanged for the purposes of this programme. Wherever possible aggregated information will be shared which does not enable individual family members to be identified.

4.2 Sensitive Personal Data

This is also defined in the Information Sharing Protocol and includes information on the commission or alleged commission of offences by the data subject, proceedings for any such offence and the disposal of such proceedings, the racial or ethnic origin of the data subject and the physical or mental health of the data subject. The Data Protection Act sets out additional safeguards for any processing of sensitive personal data. Wherever possible aggregated information will be shared which does not enable individual family members to be identified.

4.3 Information to be Shared

The data to be shared by each partner are set out in **Appendix B.** For each data set, a data extract specification will be agreed on behalf of the data controller. New data sets may be agreed with the data controller where they are compatible with the purposes of this agreement. These amendments will be discussed and agreed with the Information Manager/Information Governance Lead (Appendix E) of the relevant partners and the revised table will be dated so that the current agreed data set is apparent.

4.3.1 Identification of families for Inclusion in the Programme

In order to identify if families meet the criteria for inclusion on the Programme it will be necessary for data sets to be circulated amongst the partners. For each data set, this will be the minimum amount of data necessary to enable the matching to be undertaken accurately but with a minimum invasion of privacy. Where possible the data matching will be done electronically to minimise the disclosure of personal and sensitive personal data. As soon as data matching has been completed all information received from partners relating to individuals whose families do not meet the criteria will be deleted.

Following the identification of families meeting the programme criteria, each family will be assessed to determine what support they are already receiving and whether a multi agency approach is suitable.

4.3.2 Team around the Family

Some of the families which meet the criteria for inclusion on the Programme will already be receiving support from one or more of the partners. However, other families may need a Family Support Worker/Think Family Worker/Changing Lives Worker (Key Worker) to be allocated to the family. The Key Worker may bring together a multi-agency team around the Family. In this situation, partners will provide additional, relevant, detailed information specific to the family members and on a case by case basis directly to the key worker in order for appropriate interventions to be given. Some partners may choose to use existing multi-agency arrangements. In addition, partners not currently signed up to this ISA, but who will attend Team around the Family meetings, will exchange information under a confidentiality agreement already in use for similar joint action group (JAG) activity.

4.3.3 Evaluation of the Programme and Payments by Results

Evaluation of the Programme will be informed by consideration of the following:

- Payment by Results criteria as defined by DCLG (**See Appendix D**)
- Key national performance indicators
- Key local performance indicators

The sharing of information to support this activity will be the minimum required to inform all three elements and wherever possible this will be done without the disclosure of personally identifiable information. The precise structure of the data sets will be agreed locally to meet relevant legal requirements and available resources and will be included in the Table at **Appendix B.**

For further information see the Troubled Families Financial Framework.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/11469/2117840.pdf

The Councils are able to claim Payments by Results (PbR) as a means of funding the programme for families (households) which have been identified for inclusion on the Programme.

This anonymised information will be shared with Government departments and agencies to enable claims to be made.

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 unless they have a statutory obligation to do so or the information is also covered by another ISA.

6 Ensuring information is accurate

Partners will ensure as far as possible that the information which they supply is accurate and where the receiving partners have difficulties matching that information with information already in their possession, will assist as far as possible to ensure that the correct information is data matched.

7 Who is going to be responsible for sharing this information?

Each partner will identify their staff members who are authorised to process, extract, share and data match information for the identification of troubled families and measuring the effectiveness of the programme. Named individuals and frequency will be detailed in the data extract specifications.

8 How will the information be shared?

8.1 Electronic information

Where information is shared electronically the data will be sent by secure email (for example .GCSx .pnn .gsi. cjsm) to and from the authorised staff members associated with the management and delivery of the Programme as identified in the relevant data extract specifications. This will be the minimal information sets for identification of families for inclusion in the Programme and outcome monitoring.

8.2 Family Support Workers/ THINK Family Workers / Changing Lives Key Workers

Information sharing at Team around the Family meetings will take place as set out in section 4.3.2. **Appendix C** contains the security requirements for handling restricted and sensitive information.

9 Who will own the information?

The Chief Executive/Officer of the organisation which originally holds the information is the Data Controller. Once that information is shared with another partner under this ISA the Data Controller of the organisation receiving the information becomes the Data Controller on receipt and will be responsible for ensuring that the information is held and used securely in accordance with this purpose, relevant legislation and this Information Sharing Agreement. Where a partner is using individuals employed by another agency to process the information and deliver the Programme the partner will accept responsibility for this processing and ensure that appropriate signed contracts or agreements are in place to ensure that the conditions contained within this ISA are adhered to by these other agencies.

10 How long will it be retained by the parties?

Data will be destroyed when retention is no longer necessary for the identification of families and the provision of support, counselling and mentoring which supports the aims of the Programme, or evaluation of the effectiveness of the Programme unless agreed otherwise with the providing partner organisation. All information supplied in order to identify families for inclusion in the programme which relates to individuals who do not meet the criteria will be deleted as soon as the data matching has been completed.

Given that the Programme is due to last until at least 2015 information will need to be retained until at least this date. Within 12 months information relating to

individuals/families will be assessed and if there is no indication of further risk information will be deleted. Partners may retain a marker to indicate that the individual is a member of a family included on this Programme.

11 State the security classification of the information

The information required for the Programme is personal and sensitive personal information and should be considered to be "Restricted" when applying the security requirements in **Appendix C.**

12 Breach of confidentiality

Partners will follow the following procedure if there is a breach of this Agreement 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.

Any breaches of this Agreement must be reported to the partner providing the information at the earliest opportunity in accordance with the agreed procedure. All breaches will be recorded and investigated by the partners involved. The contact details for the post holder who should be notified for each partner is recorded in **Appendix E**. 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. Leicestershire Police will be consulted and determine whether any criminal investigation is required.

13 Indemnity

There is no requirement for an indemnity in relation to this ISA as the responsibility of Data Controller passes to the receiving partner.

14 Review of Information Sharing Agreements

This Agreement will initially be reviewed after 12 months and then as necessary following the guidance in the Information Sharing Protocol.

15 Closure/termination of agreement

Any partner organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and be evidenced. If necessary, steps will be taken to restrict access to the system as soon as possible after such a request.

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.

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

Each partner organisation shall publish 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 Data Protection Act 1998

Subject access requests and other notices relating to a data subjects rights made under the Data Protection Act 1998 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 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 subject access provisions of the Data Protection Act 1998 as they see fit.

18 Amendments

If there are any key changes to this information sharing process, this agreement should be reviewed and updated

Signature (Chief Executive/Officer): Sandra Whiles

Name: SANDRA WHILES

Post: CHIEF EXECUTIVE

Organisation: BLABY DISTRICT COUNCIL

Date: 30/1/2014

Please ensure a copy of this completed agreement is sent to the Information Management/Data Protection Sections of each organisation concerned and consult these sections if you have any queries.

Appendix A: Supporting Leicestershire Families /THINK Family/Changing Lives

Data Protection Act 1998

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 - 8 of the Data protection Act 1998. Where all 8 principles are satisfied, the sharing of information will be lawful. Therefore the requirements of each principle 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?
DUTY OF CONFIDENCE Confidentiality arising from the relationship of the data controller with the data subject. This provision restricts the data controller from using the information for a purpose other than that for which it was provided.	All partners to this agreement will have notified the Information Commissioner of their holding data under a relevant purpose. All disclosures within this agreement will be for this purpose. Partners will proactively communicate to individuals and the community at large that this sharing takes place and will deal with any specific requests for information not to be shared on a case by case basis.
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 limits of its legal powers.	The partners are relying upon the legislation in Section 3 to provide the vires to share information with the parties 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.
ARTICLES HUMAN RIGHTS Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence). There shall be no interference by a public authority with the exercise of this right except such as is in	The purposes for which the defined datasets are being shared will always satisfy one of more these conditions in particular the sharing of information will contribute to supporting public safety, promoting economic well-being, the prevention of disorder or crime and

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".	protecting of the rights and freedoms of others.
FAIR PROCESSING 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.	It is argued that where an individual is the subject of any of the sharing activities listed in this agreement, that individuals 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.
First Principle Requirements to satisfy conditions in Schedule 2 Data Protection Act 1998	How will partners satisfy these requirements? Note: Only one of the conditions needs to apply
CONSENT	Where appropriate, this information sharing will be discussed with the individual who is the subject of the information and they will be asked for their consent
LEGAL OBLIGATION The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.	Section 3 of this agreement sets out the relevant legal obligations which are exercisable by partners in support of the objectives of the programme set out in section 1.
EXERCISING LEGAL FUNCTIONS - 1 The processing is necessary for the exercise of any functions conferred by or under any enactment.	Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 1. These functions are also reflected in relevant strategy documents, for example the Community Safety Partnership Strategic Assessment and Delivery Plan. It is clearly in the public interest to

	prevent crimes and anti-social behaviour activities and other outcomes, supported by the types of sharing described within this document.
LEGITIMATE INTERESTS The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed.....	Section 3 of this agreement sets out the relevant legitimate interests which are exercisable by partners in support of the objectives of the programme set out in section 1.
PUBLIC FUNCTIONS For the exercise of any other functions of a public nature exercised in the public interest.	Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 1.
First Principle Requirements to satisfy conditions in Schedule 3 Data Protection Act 1998	How will partners satisfy these requirements? Note: Only one of the conditions needs to apply
EXPLICIT CONSENT	Where appropriate, this information sharing will be discussed with the individual who is the subject of the information and they will be asked for their explicit consent
ADMINISTRATION OF JUSTICE or EXERCISE OF A FUNCTION 7 (1) the processing is necessary - (a) for the administration of justice, (b) for the exercise of any functions conferred on any person by or under an enactment.	Section 3 of this agreement sets out the relevant legal functions which are exercisable by partners in support of the objectives of the programme set out in section 1.
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 1 (1) The processing – (a) is in the substantial public interest: (b) is necessary for the purposes of the prevention or detection of any unlawful act; and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.	Processing will only be undertaken in circumstances where it is "in the substantial public interest" e.g. in order to protect public safety and vulnerable people by identifying families which will receive support, counselling and mentoring which includes the aim of preventing involvement in further crime and ASB
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 (4) "The processing – (a) is in the substantial public interest; (b) is necessary for the discharge of any function which is designed for the provision of confidential	Processing will only be undertaken in circumstances where it is "in the substantial public interest" e.g. in order to protect public safety and vulnerable people by identifying families which will receive support, counselling and mentoring with the aim of preventing involvement in further crime and ASB

counselling, advice, support or any other service; and (c) is carried out without the explicit consent of the data subject because the processing – (i) is necessary in a case where consent cannot be given by the data subject, (ii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or (iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.	
Data Protection (Processing of Sensitive Personal Data) Order SI 2000 No 417 (10) The Processing is necessary for the exercise of any functions conferred on a constable by any rule of law	Processing will only be undertaken in order to protect public safety and vulnerable people by identifying families which will receive support, counselling and mentoring with the aim of preventing involvement in further crime and ASB

Second Principle

Second Principle Requirements	How will partners satisfy these requirements?
Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner Incompatible with that purpose or those purposes.	The information is being shared to identify families which will receive support, counselling and mentoring which includes the aim of preventing involvement in further crime and ASB so the sharing is compatible with the Purposes for which it was originally collected.

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.	Because the purposes specified are wide ranging it is not possible to be prescriptive in relation to individual data fields, forms and printouts. However, partners to this agreement will comply

	with this principle by only disclosing to each other what is needed 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. Following the receipt of evidence from partner's about a breach of an Anti-Social Behaviour Order, Anti-Social Behaviour Injunction or a bail condition, police will not action enforcement activity in respect of the subject without first verifying the currency of the order or bail condition. Note the comments below about the 5th principle.

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.	Data will be destroyed when retention is no longer necessary for the identification of families and the provision of support, counselling and mentoring, or evaluation of the effectiveness of the SLF programme unless agreed otherwise with the providing partner organisation.

Sixth Principle

Sixth Principle 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 (potentially under Section 29) of the Data Protection Act, 1998 is appropriate.

Seventh Principle

Seventh 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 App C for restricted information Police information stored on partners systems will only be available to staff who need that information to carry out the purpose.

Eighth Principle

Eighth Principle Requirements	How will partners satisfy these requirements?
Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.	Since this is a local agreement this section will not be relevant.

Appendix B

Table detailing the specific exchanges of information between the partners to this ISA as of 14th October 2013

From	To	Information	What this is to be used for	How often	How will this be provided/ retained
Leicestershire Police through IOM Disclosure Team	City TF County SLF	Full Name Dob Address in geographic areas for:- - Prolific and Priority Offenders (PPO's) - Integrated Offender Managed individuals (IOM) - Red and Amber nominal's on Police tier lists - Repeat perpetrators of domestic violence – 3 incidents in 2 week period Once identified as meeting the TF criteria a breakdown of the number of proven offences / incidences over the last 12 months broken down by month for those meeting the criteria	Identification of families to enter Programme Baseline and outcomes tracking data for Payment by Results & evaluation	Monthly Monthly	Secure email Any records which do not meet the criteria will be deleted
Leicestershire Police on behalf of the Sentinel Joint Data Controllers through IOM Disclosure Team	City TF County SLF	Full Name Addresses Dob of perpetrators of ASB incidents** and number of incidents they have been involved in over the last 12 months broken down by months	Identification of families to enter Programme. Baseline and outcomes tracking data for Payment by Results & evaluation		Secure email Any records which do not meet the criteria will be deleted
Probation IOM Disclosure Team	City TF County SLF	Full Name Dob Address in geographic areas for:- - Class A drug using parents	Identification of families to enter Programme	Monthly	Secure email

Leicester City Youth Offending Service	City TF	Full Name Address Dob Crime Outcome Decision of Panel for all Juveniles who have had a proven offence* PPOs and IOM managed in the last 12 months (broken down by number of offences per month)	Identification of families to enter Programme. Baseline and tracking of outcomes for Payment by Results & evaluation	Monthly	Internal data transfer
Leicestershire County Youth Offending Service	County SLF	Full Name Address Dob Crime Outcome Decision of Panel for all Juveniles who have had a proven offence in the last 12 months (broken down by number of offences per month)	Identification of families to enter Programme	Monthly	Internal data transfer
Leicestershire Police through IOM Disclosure Team	City TF County SLF Rutland DC Direct to Key Worker	For families who have been allocated a Key Worker only: all relevant information relating to individuals in the family * (geographical area)	Effective intervention and management	On allocation and updating as required	Secure email
Rutland DC City TF County SLF	IOM Disclosure Team	Full names Addresses Dob for families which meet their criteria / are allocated a key worker	To obtain all relevant information for key worker	On identification / allocation	Secure email
District/Borough Councils	County SLF	Name Address Dob for individuals with relevant ASB disposals ** Number of complaints	Identification of families Baseline and tracking of outcomes for Payment by Results & evaluation	Monthly	Accessed via Sentinel
IOM Disclosure Team	Rutland DC	? Brief details? Staff contacts	To obtain all relevant information for key worker	On allocation and updating as required	Secure email
Leicestershire County Council	City TF	School attendance data for city children attending county schools (including exclusions / permanent exclusions / children in PRU's)	Identification of families to enter Programme. Baseline and tracking of outcomes for Payment by Results & evaluation	Termly	Secure email

County SLF	City TF	School attendance data for county children attending city schools (including exclusions / permanent exclusions / children in PRU's)	Identification of families to enter Programme. Baseline and tracking of outcomes for Payment by Results & evaluation	Termly	Secure email
DWP / JCP	City TF County SLF	Information for families identified as meeting the criteria including; • Benefit information • Sanction information • Training & provision information • Employment information • Work Programme & ESF Programme information *as agreed in DWP data sharing template	To obtain all relevant information for key worker	Weekly	As per the separate ISA with the DWP
City TF	DWP / JCP	Full names Addresses Dob for families which meet the TF criteria / are allocated a key worker	To obtain all relevant information for key worker	Weekly	Secure email
City TF	Working Links (ESF provider)	Full names Addresses Dob for families which meet the TF criteria / are allocated a key worker	To obtain all relevant information for key worker	On allocation and updating as required	Secure email
Working Links (ESF provider)	City TF Team	For families who have been allocated a key worker only: all relevant information relating to individuals in the family	Effective intervention and management	On allocation and updating as required	
Leicestershire Partnership NHS Trust	City TF team County SLF team	For families who have been identified as meeting the TF criteria / allocated a key worker only: name and contact details of services involved with the family	To obtain all relevant information for key worker Effective intervention and management	On allocation and updating as required	Secure email
City TF team County SLF team	Leicestershire Partnership NHS Trust	Full names Addresses Dob for families which meet the TF criteria / are allocated a key worker	To obtain all relevant information for Key Worker	Weekly	Secure email
Key Worker	Multi Agency	Relevant information gathered to inform	Add additional relevant	Ad Hoc	Face to face or Secure

	Team JAG meetings.	decision making while engaging with the Troubled Families Programme.	information to Partners in-house applications to inform future interactions.		email.

* For the purposes of this programme, a 'proven offence' is any offence which receives a formal out of court or court disposal. This includes custody, fines, community sentences, youth cautions, conditional youth cautions, cautions and Penalty Notices for Disorder.

Informal disposals, such as restorative justice which are not recorded on PNC, are not included because these would require consent from the relevant individuals. Assurances would have been provided by the police at the time the information was captured that this would not be recorded onto the PNC and therefore not shared further.

** Definition of relevant ASB incidents: Where one or more member has an anti-social behaviour order, anti-social behaviour injunction, anti-social behaviour contract, or where the family has been subject to a housing-related anti-social behaviour intervention in the last 12 months (such as a notice of seeking possession on anti-social behaviour grounds, a housing-related injunction, a demotion order, eviction from social housing on anti-social behaviour grounds).

Appendix C:
Information Security Standards

1. All partners to this ISA agree to hold all information shared under it to applicable security standards. For the purpose of this ISA applicable security standards are defined as being "achieved or will be working towards ISO 27001, the International Standard for Information Security Management, compliance or a similar level of compatible security."

2. Each Partner accepts that other partners are professionally competent and it is for each partner to assess its security needs and identify what is and is not needed to comply with these.

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 the updates needed to keep this document up to date. These should be provided at least three months before such changes are due to be effective to the signatories of the ISA who will be responsible for ensuring their incorporation into the ISA; and
ii) to confirm as part of its review process that nothing has changed to the reviewing body.

5. Where Partners do not have a security classification scheme which includes handling rules, the following points should be considered:
   - Ensure that unauthorised staff and other individuals are prevented from gaining access to personal and sensitive personal data shared under this ISA
   - Ensure visitors are received and supervised at all times in areas where personal data and sensitive personal data shared under this ISA is stored
   - Ensure that all computer systems that contain personal data and sensitive personal data shared under this ISA are password-protected. The level of security should depend on the type of data held, but ensure that only those who need to use the data have access.
   - Ensure all new software is virus-checked prior to loading onto an Authority machine. Do the same for disks.

6. Where a partner organisation uses another organisation to provide a service which requires access to information shared under this ISA, they will ensure that the responsibilities for compliance with relevant legislation and security are included in the contract or agreement.

7. Ensure that staff:
   - 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 to an insecure email the personal information must be contained within a password protected attachment.
- Check that the intended recipient of a fax containing personal data is aware that it is being sent and can ensure security on delivery.
- Ensure their paper files are stored in secure locations and only accessed by those who need 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 Data Protection Act 1998 exemption.
- Do not leave personal, sensitive personal or operational information on public display in any form.
- Adhere to a Clear Desk policy. At the end of each day sensitive material must be locked away securely.

Government Protective Marking Scheme
Handling Rules Regarding Protectively Marked Material

Any information which relates to identifiable individuals or which may disclose current investigations or investigative techniques should be classified as "Restricted" and handled as instructed below.

YOUR ACTION	RESTRICTED
Storage of papers	Protected by one barrier, e.g. a locked container within a secure building/room.
Disposal of papers	Use secure waste sacks. Keep secure when left unattended.
Disposal of magnetic media	Securely destroy. All types of discs – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction.
Movement within organisation via internal dispatch	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.
Movement between partner agencies	By post or courier in a sealed envelope. Do not show protective marking on the envelope.
Organisation Data Network	May be used if network has been accredited to 'Restricted'. Your IT department should be able to advise.
Secure email between partners	Only to emails using PNN, GSI, GCSX, CJSM or MOD secure addressing conventions. Remember emails to any other address are no more secure than writing the information on a postcard.
Laptops, removable media, USB, etc	Must be owned by the employer and encrypted with the encryption approved by the Force IT department. No personally owned removable media is to be used.
Internal and public telephone network	May be used.

Mobile telephone (voice and text)	Digital cell phones may be used. Only use analogue cell phones if operationally urgent, use guarded speech and keep conversation brief.
WAP telephones	Not to be used.
Radio not 'Airwave'	Radio networks are continually monitored. Care should be taken when disclosing information of a sensitive or personal nature and if not operationally urgent another means of communication must be sought.
Pager systems	Not to be used.
Fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.

Appendix D

Supporting Leicestershire Families /THINK Ffamily/Changing lives
Payment by Results criteria as defined by DCLG

1 Crime/anti-social behaviour

Households with 1 or more under 18-year-old with a **proven*** offence in the last 12 months relating to crime or anti-social behaviour *

And/or

Households where 1 or more member has an:

- an anti-social behaviour order,
- anti-social behaviour injunction,
- anti-social behaviour contract,
- or where the family has been subject to a housing-related anti-social behaviour intervention in the last 12 months (such as a notice of seeking possession on anti-social behaviour grounds, a housing-related injunction, a demotion order, eviction from social housing on anti-social behaviour grounds1).

* A **proven** offence is any offence which receives a formal out of court or court disposal. This includes custody, fines, community sentences, reprimands, warnings, cautions and Penalty Notices for Disorder. Informal disposals, such as restorative justice which are not recorded on PNC, are not included. Formal reprimands and warnings are being replaced with effect from 1st April 2013 with youth cautions and conditional youth cautions.

2 Education

Households affected by truancy or exclusion from school, where a child:

- Has been subject to permanent exclusion; three or more fixed school exclusions across the last 3 consecutive terms;

  or

- Is in a Pupil Referral Unit or alternative provision because they have previously been excluded; OR is not on a school roll;

  And/or

- A child has had 15% unauthorised absences or more from school across the last 3 consecutive terms.

3 Adult(s) in Work

Households which also have an adult on Department for Work and Pensions out of work benefits (Employment and Support Allowance, Incapacity Benefit, Carer's Allowance, Income Support and/or Jobseekers Allowance, Severe Disablement Allowance).

4 Local Discretion

Use a local **discretion filter to add** other families who meet any 2 of the 3 criteria above **and** are a cause for concern. It is up local partners to identify, prioritise and who are **high cost** and those with health problems. These could include:

- Families containing a child who is on a Child Protection Plan or where the local authority is considering accommodating them as a looked after child
- Families subject to frequent police call-outs or arrests or containing adults with proven offences in the last 12 months, such as those who have been in prison, prolific and priority offenders, or families involved in gang-related crime
- Families with health problems (see below)

Particular priority health problems which you should consider include:

- Emotional and mental health problems
- Drug and alcohol misuse
- Long term health conditions
- Health problems caused by domestic abuse
- Under 18 conceptions

Appendix E **Information Management/Governance Contacts**

Partner	Post	Tel No	Email
Leicestershire County Council			
Leicester City Council	**Information Governance Manager**	**0116 4541300**	**lynn.wyeth@leicester.gov.uk**
Leicestershire Police	**Information Manager**	**0116 2485218**	**Anne.Chafer@leicestershire.pnn.police.uk**
County Youth Offending Services			
City Youth Offending Services			
Probation			
NHS Leicestershire Partnership Trust			
DWP			
Rutland District Council			
Blaby District Council	Contracts + Information Officer 0116 272 7558 alana.diffey@blaby.gov.uk		
Charnwood Borough Council			
Harborough District Council			
Hinckley and Bosworth Borough Council			
Melton Borough Council			
North West Leicestershire District Council	**Legal Services Team Manager**		**Dave.gill@nwleicestershire.gov.uk**
Oadby and Wigston District Council			
Working Links (City Council ESF Provider)			
Women's Aid Leicester Ltd (County Domestic Violence Service)			

Information Security Contacts

Partner	Post or SIRO	Tel No	Email
Leicestershire County Council			
Leicester City Council	**Head of Information Assurance**	**0116 4541271**	**john.doyle@leicester.gov.uk**
Leicestershire Police	**ISO**	**0116 248 5161**	**Fiona.linton@leicestershire.pnn.police.uk**
County Youth Offending Services			

City Youth Offending Services			
Probation			
NHS Leicestershire Partnership Trust			
DWP			
Rutland District Council			
Blaby District Council	As above.		
Charnwood Borough Council			
Harborough District Council			
Hinckley and Bosworth Borough Council			
Melton Borough Council			
North West Leicestershire District Council	**Information Management offi**		**Sue.wright@nwleiecstershire.gov.uk**
Oadby and Wigston District Council			
Working Links (City Council ESF Provider)			
Women's Aid Leicester Ltd (County Domestic Violence Service)			