INFORMATION SHARING AGREEMENT (ISA)

Counter Terrorism – Prevent Case Management and Channel Project

Version 12

SUMMARY SHEET

ISA Ref:	LCC 2553

PURPOSE	1. To enable the sharing of information between the Parties in order to ensure the maintenance of community safety, protection of life and property and the prevention and detection of crime and disorder. 2. To facilitate the collection and exchange of relevant information between Leicestershire Police and the Parties to prevent terrorism incorporating the Home Office Channel Project.

PARTNERS	Leicester City Council Partners as per Appendix B

Date Agreement comes into force:	When signed

Date of Agreement Review:	See 8.3

Agreement Owner:	Leicester City Council

Agreement drawn up by:	

Location of Agreement in City Council:	Community Safety

Protective Marking:	Not Protectively Marked

VERSION RECORD

Version No.	Amendments Made	Authorisation
V1.0	3 July 2001 – First draft for consultation	
V2.0	23 July 2010 – Agreed and circulated for signing.	
V2.1	Crest, front pages and version control added. GPMS marking added. Indemnity para changed. Review of ISA para added. Confidentiality Agreement para added.	
V2.2	24th August 2011 Indemnity paragraph added Confidentiality guidance added	
5 9 11	Comment re legal basis. 29(3) is not a legal basis. re whether CDA applies.	
06/09/11	Added lawful authority Added Appendix C Renamed v.5	
13/01/12	Added Appendix D Renamed Version 6	
12/02/12	Version 7 Channel Appendix A	
15/02/12	Channel Appendix amendment Chief officers names	
22/03/12	Format changes Version 8	
29/09/15	Revised draft amended and updated	
03/12/2015	Re-named Version 10 Reference to statutory duty of CTSA and Channel/PCM guidance. Leicestershire Police – name and crest updated 'Partners' to agreement updated as 'Designated Prevent Co-Ordinators' Inclusion of cases that are discussed at Channel Group and managed under Prevent Case Management	

	'Gold Group' amended to 'Prevent Steering Group' and 'Silver Group' amended to 'Channel Group' Expectation that 'Designated Prevent Co-Ordinators' will be SC cleared Addition of EMAS, Leicester University, De Montfort University and Loughborough University to list of Partner, Appendix B signatories and Designated Officers	
01/10/16	Re-named Version 11 Amended Title to reflect Prevent Case Management Amended logo from Leicestershire Police to Leicester City Council Amended agreement owner to Leicester City Council Amended agreement location to Leicester City Council Removed East Midlands Ambulance Service (EMAS) as designated Prevent Co-ordinator Removed Leicester University as designated Prevent Co-ordinator Removed De Montfort University as as designated Prevent Co-ordinator Removed Loughborough University as designated Prevent Co-ordinator Amended references to 'Channel Project' to Channel Programme Included references to Prevent Case Management Amended Appendix A to include Counter Terrorism and Security Act 2015 Amended Signatories in Appendix A to reflect current partnership members Removed attendance list template Removed Appendix E – data consent form	
09/04/23	Version 12 Revised to update to UK GDPR terminology. Update NHS CCGs to be re-named ICB Additional sharing powers listed.	

Introduction

This Information Sharing Agreement has been developed to support the multi-agency partnership involvement in Counter Terrorism and is intended to operate within existing information sharing principles whilst providing a level of detail of Counter Terrorism activity.

This ISA supports the aims of the Prevent Statutory Duty issued for specified authorities in England and Wales on the duty in the Counter Terrorism and Security Act 2015 to have due regard to the need to prevent people being drawn into terrorism. It also supports both the Channel Programme and Prevent Case Management Guidance.

The aim of this Agreement is to enable the sharing of information between the Parties in order to ensure the maintenance of community safety, protection of life and property and the prevention and detection of crime and disorder.

This agreement will incorporate the Channel Programme which is intended to contribute to the aim of the Prevent Strand of the Home Office Counter Terrorism Strategy 'Contest' – to prevent terrorism by helping individuals to resist any process intended to cause them to become violently extreme and by disrupting the recruitment activities of extremists. It is a community-based initiative, which aims to utilise partnership working between the police, local organisations and communities, to respond to community concerns regarding radical or extreme views.

This Agreement sets out the legal provisions relating to personal data sharing and takes account of the relevant Codes of Practice in respect of the sharing of personal data held by the Parties including but not limited to the Management of Police Information Guidance and the ACPO Data Protection Manual of Guidance and the ACPO Channel Project Guidance Manual.

This Agreement contains details of the standards agreed by the Parties involved in the sharing of personal data and personally identifiable information so as to maintain confidentiality, integrity and compliance with the data protection principles, whilst ensuring that information is shared with those who 'need to know'.

Requests for information from any of the Parties to the Agreement should be considered on a case by case basis in light of this Agreement and the relevant legal parameters identified concerning the sharing of such personal data.

Information should not be disclosed to any persons who are not Parties to this Agreement, identified below, or if there is any doubt that the elements of this Agreement are not in place, might be breached or not adhered to.

1. Partners

1.1 The Designated Prevent Co-Ordinators to this Agreement are:

Leicestershire Police
Leicester City Council
Leicestershire County Council

Leicestershire Probation Service
Leicestershire Prison Service
Leicestershire Partnership NHS Trust
University Hospitals of Leicester NHS Trust
Leicester, Leicestershire and Rutland Integrated Care Board
NHS England (Midlands and East)

1.2 It will be the responsibility of these signatories to ensure that:

- Realistic expectations prevail from the outset;
- Ethical Standards are maintained;
- A mechanism exists by which the flow of information can be controlled;
- Appropriate training is provided;
- Adequate arrangements exist to test adherence to the Agreement; and
- Data Protection and other relevant legislative requirements are met.

2. Purpose of this Agreement

2.1 The purpose of this Agreement is to enable the disclosure of information between the Parties in accordance with the aims of Prevent Case Management and the Channel Programme. The Channel Programme supports the Home Office Prevent Strategy, in 'preventing terrorism by helping individuals to resist processes designed to turn them to violently extreme behaviour.'

2.2 Specifically, it aims to identify individuals and networks that are turning to violent extremisms or who are vulnerable to becoming so and those individuals and networks that seek to turn others to such behaviour, to enable measures to be developed aimed at facilitating the delivery of effective interventions and so divert vulnerable persons from turning to violently extreme behaviour.

2.3 The direct purpose of the Channel Programme is in accordance with the policing purpose as defined in the Code of Practice for the Management of Police Information:

- Protecting life and property
- Preserving order
- Preventing the commissioning of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law.

3. Details of the Information to be Exchanged

3.1 It is recognised that for the purposes of this Agreement, that it may be necessary for the Partners to share information which constitutes personal data and special category personal data under the provisions of the UK GDPR and the Data Protection Act 2018.

3.2 Where appropriate, anonymised information will be supplied to the Prevent Steering Group, providing them with sufficient information to enable generic intervention methods to be considered. In higher risk cases it may be appropriate to share sensitive personal data to better inform Prevent Steering Group's decision making. This is particularly relevant where failure to provide immediate interventions may involve significant loss of public confidence.

3.3 An example of anonymised data may be: “A Juvenile male has been highlighted through an immigration interview to be a vulnerable risk, having been subjected to violent extremism in his home country. This male has been placed in an educational establishment that has opposing religious groups within it.”

3.4 From this meeting a Channel Group meeting will be convened involving the Channel Project Co-ordinator (Police) and any other relevant strategic partner practitioner identified by the Prevent Steering Group for this intervention. At this point ‘sensitive personal data’ will be disclosed which may include; name, date of birth, address, ethnicity and an intelligence summary. This disclosure will only be retained in document form by the Channel Project Co-ordinator.

3.5 At the Channel Group meeting ‘sensitive personal data’ will be disclosed to relevant strategic partners as determined by the specific intervention required in each case. An example of this may be; “Thomas Smith born 01/01/01 who resides in the care home at Smithfield’s Crescent. A Muslim male has been viewing Al Qaeda extremist websites whilst at Smithfield’s School”. Smith has previous convictions for violence and robbery from 2007 to 2008 and is believed to have mental health issues. The Channel Group will also discuss vulnerable individuals who do not meet the threshold to be adopted into Channel but who are managed under Prevent Case Management.

3.6 This special category and sensitive personal data will only be retained in document form by the Channel Project Co-ordinator. Those individuals may record such information as is required to undertake their official duties to respond to the Prevent Agenda, and take specific action in respect of the identified individual. Such information will be recorded in accordance with the respective organisation’s policy and procedure.

3.7 At the relevant intervention meeting actions will be discussed and prioritised. Each panel member has a responsibility to create a file or folder record of each individual action and result accordingly. It must include copies of the tasking, details of the data accessed and notes of any meeting, correspondence or phone calls relating to the request.

3.8 A comprehensive record must be made of all decisions.

3.9 The Channel Co-ordinator will ensure these decisions are centrally recorded.

3.10 Under the direction of the Leicester, Leicestershire and Rutland Prevent Steering Group information may be disclosed to relevant approved individuals who agree to deliver intervention assistance on behalf of the Partnership. An example of this may be “Thomas Smith a 12 year old male who attends the Smithfield Mosque has been viewing extremist websites. Could you work with the Channel Programme and intervene by offering Smith an alternative faith view point.”

3.11 On a case by case basis consideration will be given as to whether information can be anonymised and provided in a depersonalised format. Any sensitive personal data will only be shared where it is necessary to do so in order to consider an intervention, as set out within the Channel Programme Guidance.

3.12 The disclosure of information must only take place where it is valid and legally justified.

4. Fair and Lawful Processing

4.1 In order to satisfy the first Data Protection principle, personal data must be processed fairly and lawfully and shall not be processed unless at least one of the Article 6 conditions is met and in the case of special category personal data, at least one of the Article 9 conditions is also met. These requirements are described below.

4.2 Lawful Processing

The information exchanged within this information sharing agreement must:

- Have lawful authority
- Be necessary and proportionate

4.2.1 Lawful Authority

Channel is *not* a process for gathering intelligence. But, in common with other programmes, it does require the sharing of personal information about people at risk. Information sharing must be assessed on a case by case basis and governed by legislation, the details of which are set out in Annex A

Each Partner or body acting on behalf of such Partner, sharing information must have prima facie statutory or common law duty to do so. Information may be shared under the following provisions:

Counter Terrorism and Security Act 2015

The legal basis for sharing data as specified above is by virtue of section 26 of the Act. Parties listed in this Agreement are 'specified authorities' as defined in Schedule 6 of the Counter Terrorism and Security Act 2015.

Crime and Disorder Act 1998

The Crime and Disorder Act introduces measures to reduce crime and disorder. Specifically, Section 115 of the Act provides a power, but not an obligation, for information sharing between ‘responsible’ public bodies and with ‘co-operating’ bodies participating in the formation and implementation of the local crime and disorder strategy to pursue specific objectives as defined in this Agreement.

This power must be exercised in accordance with any other relevant legislation, including the Human Rights Act 1998, the UK GDPR and the Data Protection Act 2018.

The responsibility for any disclosure will remain with the agency that holds the data.

Where it is necessary for the purpose of preventing and detecting crime or the apprehension or prosecution of offenders, personal data may be shared in circumstances where the non-disclosure of information would be likely to prejudice that purpose.

For further Gateways, exemptions and explicit powers See Channel Supporting individuals vulnerable to recruitment by violent extremism Annex A Sharing information with partners – Gateways, exemptions and explicit powers.

4.2.2 Necessity

The information will be shared where necessary for the purpose of preventing terrorism by helping individuals to resist any process intended to cause them to become violently extreme and by disrupting the recruitment activities of extremists.

4.2.3 Proportionality

To justify the proportionality of information shared it must be shown that:

- The assessment and management of risks posed by an individual could not be effectively achieved other than by sharing the information in question.
- The disclosure of the information is a proportionate response to the need to protect a person or persons.
- The procedures outlined in this Agreement would ensure compliance with Article 8 of the Human Rights Act 1998.

4.3 Fair processing

The information exchanged within this information sharing agreement must be processed fairly. Wherever possible any consequences of the processing to the individual should be taken into consideration.

4.3.1 Consent

For the purposes of this Agreement consent is considered to be;
'Any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed'

4.3.2 Consent from the data subject in respect of intervention work for sharing between the Partners will be obtained wherever possible and recorded as appropriate. Partners may consider sharing personal information with each other for *Prevent* purposes, subject to a case by case basis assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being necessary, proportionate and lawful"

4.3.4 When considering the legal powers associated with information sharing cognisance should be given to whether it is reasonable to gain full consent of the data subject. In circumstances where consent is refused or it is not reasonable to seek consent, but where it is critical that intervention takes place in accordance with the policing purpose, information may be shared where the following conditions have been met:

4.3.5 The processing is necessary in order to protect the interests of the data subject by helping them to resist any process intended to cause them to become violently

extreme and by disrupting the recruitment activities of extremists. The processing is deemed necessary:

a) In order to protect the vital interests of the data subject or another person in a case where:
   i. Consent cannot be given by or on behalf of the data subject

   or

   ii. The data controller cannot be reasonably be expected to obtain the consent of the data controller

b) In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4.3.6 Statutory Instrument (SI 2000/417) specifies further conditions under which sensitive personal information can be processed, including conditions where the processing must necessarily be carried out without the explicit consent of the data subject. Of particular relevance to Prevent are paragraph 1 (for the purposes of prevention or detection of crime), and paragraph 4 (for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service).

4.3.7 Common law powers - Because the range of partners with whom the police deal has grown – including the public, private and voluntary sectors, there may not be either an implied or explicit statutory power to share information in every circumstance. This does not necessarily mean that police cannot share the information, because it is often possible to use the common law. The decision to share using common law will be based on establishing a policing purpose for the activity that the information sharing will support, as well as an assessment of any risk. The Code of Practice on the Management of Police Information (MoPI) defines policing purposes as: protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law.

4.3.8 Disclosure of an individual's personal data engages rights under Article 8 of the European Convention on Human Rights. This provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' Whilst this right is not absolute, any interference with it must be justified. In order to justify interference, the Parties to this Agreement will need to show that it is:

- In accordance with the law
- In the pursuit of a legitimate aim; and
- Necessary in a democratic society

5. How the information may be used

5.1 It is recognised that for the purposes of this Agreement, it is necessary for both Parties to share information, which constitutes 'personal data' and possibly 'sensitive personal data' under the provisions of the UK GDPR and the Data Protection Act 2018.

5.2 The information will be used to respond to community concerns regarding radical or extreme views by assessing an individual's vulnerability to becoming violently extreme or, an individual's influence in radicalising others to violent extremism.

5.3 Personal data obtained under this Agreement may only be used for the agreed purpose and must not be further processed in any manner incompatible with the identified purpose(s).

5.4 No secondary use or other use may be made unless the consent of the disclosing Party is sought and granted.

6. Terms of Use of the Information

6.1 The information will be used solely for the Purpose set out at Section 2 above.

6.2 The data must be treated as RESTRICTED and will not be divulged or communicated to any third Parties without the written consent of the Party that provided the information.

6.3.1 Access to the data will be restricted to those employees of the Parties and approved by the nominated representative of each Party to the Agreement.

6.3.2 Transfer of data will be in the format agreed by the organisation that holds the original data.

7. Data Quality

7.1 The identity of the originator must be recorded against the relevant data.

7.2 Information shared must be fit for purpose, which means that it must be adequate, relevant and not contain excessive detail which is beyond that required for the agreed Purpose.

7.3 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 the data and notifying all other recipients of the information who must ensure that necessary corrections are made.

7.4 Appropriate records will be kept to record the sources of information to provide for this.

8. Information Retention, Review and Disposal

8.1 Each Party will maintain an auditable record of all information disclosed.

8.2 All records made will be supplied to the Channel Programme Co-ordinator in order for a single comprehensive record to be retained.

8.3 Retention periods will be agreed in a case by case basis and reviewed in accordance with relevant review dates. Records will be retained for five years.

8.4 Information will be disposed of securely in line with the records management policies of each Party.

8.5 Information no longer required for the agreed Purpose will be disposed of in a manner consistent with the security obligations defined below.

9. Information Security

9.1 General

9.1.1 Each Data Controller has obligations relating to the security of data in his control under the UK GDPR and The Data Protection Act 2018.

9.1.2 The Partners to this Agreement acknowledge the security requirements of the UK GDPR and the Data Protection Act 2018 applicable to the processing of the information subject to this Agreement.

9.1.3 Each Partner will ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

9.1.4 In particular, each Partner shall ensure that measures are in place to do everything reasonable to:

- Make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport,
- Deter deliberate compromise or opportunist attack,
- Dispose of or destroy the data in a manner to make reconstruction unlikely;
- Promote discretion in order to avoid unauthorised access.

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

9.1.6 Any suspected breach or threat to the security of the information will be reported to all relevant Parties, via the designated officer without delay.

9.2 Additional Security Requirements

9.2.1 It is envisaged that relevant information will be provided verbally during the course of Channel Programme panel meetings. Arrangements should be made for such meetings to take place in a suitably secure venue, where discussions may not be overheard. The Designated Prevent Co-Ordinators to this agreement will be required to have SC clearance.

9.2.2 Information may be made available by telephone in cases of emergency, for example, where there is a risk of immediate threat or danger to the public. Where this occurs, the information must be recorded in the members Channel Programme file or folder. Where such information sharing takes place via telephone, the identity of the caller must be satisfied.

9.2.3 All information that is shared should be done as per the 'RESTRICTED' column in Appendix D.

10. General Management of Agreement

10.1 Designated Officers

10.2 Details of the designated officers with day to day responsibility for the management of this Agreement are provided at Appendix B.

11. Individual Rights to Access Information Exchanged (Subject Access)

11.1 Any person receiving a request for information under the provisions of the Data Protection Act 1998 or Freedom of Information Act 2000 must refer the request to the relevant official in the organisation in accordance with local policy and procedures and without delay.

11.2 Where a request for information includes that information provided by the Partner organisation, the originating organisation will be consulted in accordance with normal protocols.

12. Complaints Procedure

12.1 All complaints and breaches relative to this Agreement should be referred to the signatory of the relevant organisation who will take appropriate action.

12.2 Complaints or breaches will also be notified to the designated Data Protection Manager of the relevant organisation in accordance with their respective policy and procedures.

12.3 Complaints from data subjects will be investigated first by the organisation receiving the complaint. Actions which affect other Partners will not be taken without the consent of all Parties to this agreement.

12.4 The signatories will give all reasonable assistance as is necessary to the relevant Data Controller to enable him to:

- Comply with a request for subject access
- Respond to an Information Notices served by the Information Commissioner
- Respond to complaints from the data subject
- Investigate any breach of the Agreement.

13. Confidentiality Agreement

The parties to this Agreement understand that in keeping with government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the Crime and Disorder Act 1998, it is likely that there will be individuals present at certain meetings who are not employed by an organisation who are signatories to the Information Sharing Protocol and therefore are not in a position to sign this Agreement due to the liability of the indemnity. A meeting attendance list and confidentiality agreement will be provided at each meeting and should be signed by each attendee.

It is best practice for the Confidentiality Statement to be incorporated with the attendance list to ensure full compliance with legislation. The responsibility for

ensuring that this takes place and for retaining the signed copies lies with the Chair of the meeting.

14. Indemnity

14.1 Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

14.2 It is likely that there will be individuals present at certain meetings who are not employed by an organisation who are signatories to the Leicestershire Information Sharing Protocol and therefore are not in a position to sign this Agreement due to the liability of the indemnity. The chair of the meeting will remind the individual of the need for confidentiality in relation to the issues discussed before being asked to sign a Confidentiality Agreement form. See Appendix C

15. Review of the Information Sharing Agreement

This Agreement will initially be reviewed with any reissued Channel guidance and then as necessary following the guidance in the LLR Information Sharing Protocol.

16. Termination of the Agreement

16.1 Any Party to this Agreement may at any time in writing terminate the Agreement if any Party is in material breach of any obligation under the Agreement.

16.2 Written notice should be provided by either Party regarding the termination of the Agreement.

16.3 A Partner may suspend these arrangements in order to investigate and resolve any serious breach of this Agreement.

16.4 Any such action will be notified in writing to the other Partner with immediate effect.

16.5 Partners will make every effort to resolve any dispute affecting the ability to share information under this Agreement within 30 days.

16.6 The obligations of or confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

Appendix A – Annex A – Sharing Information with Partners – Channel – A guide to local partnerships

Principles of information sharing

Effective information sharing is key to the delivery of *Prevent*, so that partners are able to take appropriately informed action. This will sometimes require the sharing of personal information between partners; this is particularly the case for Objective 3 of the *Prevent* Strategy, where sharing of information will be central to providing the best support to vulnerable individuals.

Key principle

Partners may consider sharing personal information with each other for *Prevent* purposes, subject to a case by case basis assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being necessary, proportionate and lawful. Any sharing of personal or sensitive personal data should be considered carefully, particularly where the consent of the individual is not to be obtained. The legal framework within which public sector data sharing takes place is often complex, although there is a significant amount of guidance already available. It is considered good practice to have an Information Sharing Agreement in place at local level to facilitate the sharing of information. In addition to satisfying the legal and policy requirements (see below), there are some principles which should guide *Prevent* information sharing. Necessary and proportionate

The overriding principles are necessity and proportionality. It should be confirmed by those holding information that to conduct the work in question it is necessary to share the information they hold. Only the information required to have the desired outcome should be shared, and only to those partners necessary. Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an individual or the public. Consideration should also be given to whether discussion of a case is possible with anonymised information, for example, referring to “the young person” without the need to give the individual’s name, address or any other information which might identify them.

Each case should be judged on its own merits, and the following questions should be considered when sharing information:

- What information you are intending to pass
- To whom you are intending to pass the information
- Why you are intending to pass the information (i.e. with what expected outcome)
- The legal basis on which the information is to be passed.
- Consent.

The default should be to consider seeking the consent of the individual to share information. There will, of course, be circumstances in which seeking the consent of the individual will not be desirable or possible, because it will prejudice delivery of the intended outcome, and there may be gateways or exemptions which permit sharing to take place without consent. If you cannot seek or obtain consent, or consent is refused, you cannot share personal information without satisfying one of the gateway or exemption conditions. Compliance with the Data Protection Act and Human Rights Act are significantly simplified by having the subject’s consent. The Information Commissioner has indicated that consent should be informed and unambiguous, particularly in the case of sensitive personal information. If consent is sought, the individual should understand how their information will be used, and for what purpose.

Power to share
The sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the UK GDPR, the Data Protection Act 2018, the Human Rights Act and the common law duty of confidentiality. Some statutes confer an express power to share information for a particular purpose (such as section 115 of the Crime and Disorder Act 1998).

More often, however, it will be possible to imply a power to share information because it is necessary for the fulfilment of an organisation's statutory functions. The power to share information arises only as a consequence of an organisation having the power to carry out an action which is dependent on the sharing of information. Having established a power to share information, it should be confirmed that there are no bars to sharing information, either because of a duty of confidentiality or because of the right to privacy enshrined in Article 8 of the European Convention on Human Rights.

Finally, it will also be necessary to ensure compliance with the Data Protection Act, either by meeting the processing conditions in Schedules 2 and 3, or by relying on one of the exemptions (such as section 29 for the prevention of crime). Further details of the overarching legislation and some potentially relevant gateways are set out below. Where non-public bodies (such as community organisations) are involved in delivery of *Prevent* work, you may need to pass personal and sensitive information to them and your approach to information sharing should be the same – i.e. that it is necessary, proportionate and lawful. In engaging with non-public bodies to the extent of providing personal information, it is good practice to ensure that they are aware of their own responsibilities under the Data Protection Act.

Vetting
Sharing information to prevent violent extremism should not be impeded by issues surrounding vetting. If there is a requirement for the sharing of material above restricted level the need for vetting need not be a barrier. Practitioners should consider ways to share the information which needs to be shared to enable partners to provide the necessary response. Consideration about whether it is appropriate for an individual to be vetted should be decided at a local level and on a case-by-case basis, depending on requirement and necessity.

Legislation and guidance relevant to information sharing
Although not an exhaustive list, the following acts and statutory instruments may be relevant. The original legislation can be found at the Statute Law Database (http://statutelaw.gov.uk/).

UK GDPR and Data Protection Act (DPA) 2018
The UK GDPR and the DPA are the principal pieces of legislation governing the process (including collection, storage and disclosure) of data relating to individuals. The legislation defines personal data (as information by which an individual can be identified (ether on its own or with other information)) and special category personal data (including information about an individual's health, and political or religious views), and the circumstances in and extent to which they can be processed. The legislation also details the rights of data subjects. All of the six Data Protection Principles must be complied with when sharing personal data but the first data protection principle is particularly relevant.

The first data protection principle states that personal data shall be processed:

1. Fairly
2. Lawfully (meaning that there is the power to share and other statutory and common law obligations must be complied with), and transparently
3. Only if a condition in Article 6 and, if special category personal data is involved, Article 9 is met.

All three of these requirements must be met to comply with the first data protection principle. The UK GDPR and DPA cannot render lawful any processing which would otherwise be unlawful. If compliance with the Data Protection Principles is not possible, then one of the exemptions (such as the prevention of crime of the Data Protection Act 2018) may apply.

Data Protection (Processing of Sensitive Personal Data) Order 2000
This Statutory Instrument (SI 2000/417) specifies further conditions under which sensitive personal information can be processed, including conditions where the processing must necessarily be carried out without the explicit consent of the data subject. Of particular relevance to *Prevent* are paragraph 1 (for the purposes of prevention or detection of crime), and paragraph 4 (for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service). The first data principle states that personal data shall be processed fairly and lawfully, meaning that other statutory and common law obligations must be complied with, and that the DPA cannot render lawful any processing which would otherwise be unlawful. Schedules 2 and 3 of the Act provide the conditions necessary to fulfil the requirements of the first principle.

Human Rights Act (HRA) 1998 Article 8
The European Convention on Human Rights (which is given effect by the HRA) provides that “everyone has the right to respect for his private and family life, his home and his correspondence”, and that public authorities shall not interfere with “the exercise of this right except such as 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”.

Common Law duty of confidentiality
The key principle built up from case law is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Case law has established that exceptions can exist “in the public interest”; confidentiality can also be overridden or set aside by legislation.

The Department of Health has produced a code of conduct concerning confidentiality, which is required practice for those working within or under contract to NHS organisations.

Gateways, exemptions and explicit powers Crime and Disorder Act 1998
Section 115 confers a power to disclose information to a “relevant authority” on any person who would not otherwise have such a power, where the disclosure is necessary or expedient for the purposes of any provision of the Act. The “relevant authority” includes a chief officer of police in England, Wales or Scotland, a police authority, a local authority, a health authority, a social landlord or a probation board in England and Wales. It also includes an individual acting on behalf of the relevant authority. The purposes of the Crime and Disorder Act include, under section 17, a duty for the relevant authorities to do all that they reasonably can to *prevent* crime and disorder in their area.

Common law powers
Because the range of partners with whom the police deal has grown – including the public, private and voluntary sectors, there may not be either an implied or explicit statutory power to share information in every circumstance. This does not necessarily mean that police cannot share the information, because it is often possible to use the common law. The decision to share using common law will be based on establishing a policing purpose for the activity that the information sharing will support, as well as an assessment of any risk. The Code of Practice on the Management of Police Information (MoPI) defines policing purposes as: protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law.

Local Government Act 1972 Section 111
Provides for local authorities to have "power to do anything…which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions".

Local Government Act 2000 Section 2(1)
Provides that every local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the economic, social or environmental wellbeing of the area.

Localism Act 2011 Section 1
Provides for a local authority has power to do anything that individuals generally may do.

National Health Service Act 2006 and Health and Social Care Act 2001
Section 251 of the NHSA and Section 60 of the HSCA provides a power for the Secretary of State to make regulations governing the processing of patient information.

Offender Management Act 2007
Section 14 of the OMA enables disclosure of information to or from providers of probation services, by or to Government departments, local authorities, Youth Justice Board, Parole Board, chief officers of police and relevant contractors, where the disclosure is for the probation purposes (as defined in section 1 of the Act) or other purposes connected with the management of offenders.

Counter Terrorism and Security Act 2015
Part 5 of the CTSA sets out the statutory duty on specified authorities to, in the exercise of its functions, show due regard to the need to prevent people from being drawn into terrorism.
http://www.legislation.gov.uk/ukpga/2015/6/part/5/enacted

Appendix B Signatories

Name	
Position	**Chief Constable, Leicestershire Police**
Signature	_____
Name	
Position	**Chief Operating Officer Leicester City Council**
Signature	_____
Name	
Position	**Chief Executive, Leicestershire County Council**
Signature	_____
Name	
Position	**Chief Executive, National Probation Service, Leicester Leicestershire and Rutland**
Signature	_____
Name	**HMP Leicester**
Position	**Governor**
Signature	_____
Name	**University Hospitals of Leicester NHS Trust**
Position	**Head of Safeguarding**
Signature	_____

Name
Position **Deputy Director of Nursing and Quality, Leicestershire**
Leicestershire Partnership NHS Trust

Signature _____

Name
Position **Deputy Chief Nursing Officer**
NHS Leicester, Leicestershire and Rutland Integrated Care Board
(NHS LLR ICB)

Signature _____

Name **NHS England and NHS Improvement Midlands**

Position **Assistant Director for Safeguarding**

Signature _____

Designated Officers

	Leicestershire Police
	Leicestershire County Council
	Leicester City Council
	Leicestershire Probation Service
	HM Prisons
	Leicestershire Partnership NHS Trust
	University Hospitals of Leicester NHS Trust
	LLR ICB
	NHS England, Midlands and East

CONFIDENTIALITY GUIDANCE

Appendix C

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the UK GDPR, the Data Protection Act 2018, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Common Law Duty of Confidentiality, all attendees are asked to agree to the following. This agreement will be recorded in the minutes.

- Information may be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.

- A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the subjects' confidentiality and a breach of the confidentiality of the agencies involved.

- All documents exchanged should be marked 'restricted – not to be disclosed without consent'. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.

- If further action is identified, the agency/ies that are involved with that action should retain possession of whatever information is required to assist them to proceed with the action(s) and should then make formal requests to or meet with any other agencies holding such personal information as may be required to progress the action quoting their legal basis for requesting such information outside of the meeting. No other party should use information exchanged during the course of this meeting.

- If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting and a decision will be made on the lawfulness of the disclosure. Such as the prevention or detection of crime, apprehension or prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

Appendix D

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.

If the information about an individual is such that disclosure of the information would be likely to cause a risk to the safety of the individual or if the investigation is covert this should be classified as 'CONFIDENTIAL' and handled as instructed below.

YOUR ACTION	RESTRICTED	CONFIDENTIAL
Storage of papers	Protected by one barrier, e.g. a locked container within a secure building/room	Protected by two barriers e.g. a locked container in a locked room, within a secure building
Disposal of papers	Use secure waste sacks/ confidential waste/shredding. **Keep secure when left unattended**	Downgrade by tearing into small pieces and place in secure waste sacks, or use a cross cut shredder. **Keep secure when left unattended**
Disposal of magnetic media	Securely destroy Floppy disk – dismantle and cut disk into quarters (at least), dispose with normal waste. CD ROMs – destroy completely – disintegrate, pulverise, melt or shred	Securely destroy Floppy disk – dismantle and cut disk into quarters (at least), dispose with normal waste. CD ROMs – destroy completely – disintegrate, pulverise, melt or shred
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.	In a new sealed envelope with protective marking shown Transit envelopes **must not** be used.

YOUR ACTION	RESTRICTED	CONFIDENTIAL
Movement between partner agencies	By post or courier in a sealed envelope. **Do not show** protective marking on the envelope.	By post or courier Double enveloped and both fully addressed. Protective marking shown on inner envelope only. Return address on **outer** envelope.
Organisation Data Network	May be used if network has been accredited to 'Restricted'. Your IT dept should be able to advise	May be used in conjunction with CESG Enhanced Grade Encryption.
Email between partners	Only to emails using PNN, CJSM or MOD secure addressing conventions. Remember emails to any other address are no more secure than writing the information on a postcard.	Not to be used.
Internal and public telephone network	May be used.	Only if operationally urgent. Use guarded speech and keep conversation brief.
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.	Digital cell phones may be used but only if operationally urgent Use guarded speech and keep conversation brief.
WAP telephones	Not to be used.	Not to be used.

YOUR ACTION	RESTRICTED	CONFIDENTIAL
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.	Only if operationally urgent. Use guarded speech and keep conversation brief. *
Pager systems	Not to be used.	Not to be used.
Fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.	Use secure fax machine only.

If organisations do not find it possible to apply the appropriate security this should be discussed with the originator.