Leicester, Leicestershire and Rutland Multi-Agency Overarching Safeguarding

INFORMATION SHARING AGREEMENT AND GUIDANCE

Date of Publication:	To be confirmed	
Date of Review:	12 months from date of sign last off	
Document Version Control		
Version	**By**	**Comments**
1.01 (Draft)	Sam Kirkland/Kevin Turner	Changes made to include both Children and Adult Safeguarding as a singular approach to Information Sharing
1.02 (Draft)	Sam Kirkland	Minor changes following initial comments
1.03 (Draft)	Jan Harrison	Highlighted areas pages: 17:29:33 where the reference to 'consent' needs to be replaced by ''Notify''
1.04 (Draft) July 2019	Sam Kirkland/Kevin Turner	Additional changes following July 2019 meeting
1.05 (Draft) November 2019	Sam Kirkland	Additional changes following November 2019 meeting with Safeguarding leads
1.06 (Draft) December 2019	Sam Kirkland	Dec 2019 Incorporating changes from the Police and additional guidance for practitioners
1.07 (Draft) Sept 2020	Sam Kirkland	Incorporating all comments from partners
1.08 (Draft) Dec 2020	Sam Kirkland	Incorporating changes made to 'Working Together 2018' GDPR and information sharing update
1.09 (Draft) to 1.13 (Draft) Jan 2021 to March 2021	Chris Tew	Incorporated changes during the signup process to highlight individual agencies processes
1.14 (Draft) March 2021	Chris Tew	Sign up table updated

1.15 April 2021	Chris Tew	Bridge East Midlands name updated
1.16 July 2021	Chris Tew	Sign up table updated with CCG
1.17 Aug 2021	Sam Kirkland	Update of legislation following Brexit
1.18 Feb 2022	Sam Kirkland	Review against all legislation and in line with expected review period. No material changes
1.19 April 2022	Chris Tew	Sign up table updated & logo's added
2.0 July 2022	Chris Tew	Published
2.01 September 2022	Chris Tew	CCG references changed to ICB
2.02 November 2022	Chris Tew	Amended Child death and CDOP
2.03 April 2023	Hannah Plowright and Sarah Ratcliffe	Viewed and approved latest version

Contents Page

Signatories to the Agreement

Partners	Addresses
Local Authorities	
Leicestershire County Council	County Hall, Glenfield, Leicester, LE3 8RA
Leicester City Council	City Hall, 115 Charles Street, Leicester, LE1 1FZ
Rutland County Council	Catmose, Park Rd, Oakham, Rutland, LE15 6HP
Police	
Leicestershire Police	Force Headquarters, St Johns, Enderby Leicester, LE19 2BX
Health Agencies/Organisations	
NHS Leicester, Leicestershire, and Rutland Integrated Care Board (ICB)	County Hall, Glenfield, LE3 8RA
NHS England and NHS Improvement – Midlands	Fosse House, 6 Smith Way, Grove Park, Enderby, Leicestershire, LE19 1SX
University Hospitals of Leicester NHS Trust	Level 3, Balmoral Building, Leicester Royal Infirmary, Infirmary Square, Leicester, LE1 5WW
Leicestershire Partnership NHS Trust	Unit 2, Bridge Park Plaza, Bridge Park Road, Thurmaston, LE4 8BL
East Midlands Ambulance Service NHS Trust	1 Horizon Place, Mellors Way, Nottingham Business Park, Nottingham, NG8 6PY
Probation & Prisons Agencies/Organisations	
HM Prison & Probation Service	National Probation Service, 1 Victoria Square, Birmingham, B1 1BD
HM Prison Leicester	Her Majesty's Prison and Probation Service HMP Leicester 116 Welford Road Leicester LE2 7AJ
Fire & Rescue	
Leicestershire Fire & Rescue Service	12 Geoff Monk Way, Birstall, Leicester, LE4 3BU

District Councils	
Blaby District Council	Council Offices, Desford Road, Narborough, Leicestershire, LE19 2EP
Charnwood Borough Council	Southfield Rd, Loughborough, Leicestershire, LE11 2TN
Harborough District Council	The Symington Building, Adam and Eve St, Market Harborough, Leicestershire, LE16 7AG
Hinckley and Bosworth Borough Council	Hinckley Hub, Rugby Road, Hinckley, Leicestershire, LE10 0FR
Melton Borough Council	Parkside, Burton Street, Station Approach, Melton Mowbray, Leicestershire, LE13 1GH
North West Leicestershire District Council	Councils Offices, Whitwick Road, Coalville, Leicestershire, LE67 3FJ
Oadby and Wigston Borough Council	Council Offices, Station Road, Wigston, Leicestershire, LE18 2DR
Other Agencies/Organisations	
Rainbows	Rainbows Hospice, Lark Rise, Loughborough, Leicestershire, LE11 2HS
ADHD Solutions CIC	St Gabriel's Community Centre, Kerrysdale Avenue, Leicester, LE4 7GH
Barnardo's Central England Region	Unit 6, Westleigh Business Park, Winchester Avenue, Blaby
The Bridge (East Midlands)	The Bridge, 38 Leicester Road, Loughborough, Leicestershire, LE11 2AG
Y.M.C.A.	7, East Street, Leicester, LE1 6EY
LOROs	Groby Road, Leicester LE3 9QE
Turning Point	2, Eldon Street Leicester, LE1 3QL
CFF (Centre for Fun and Families Ltd)	177/179 Narborough Road, Leicester
Living Without Abuse	7-9 Fennel Street, Loughborough, LE11 1UQ

Section 1 – Information sharing guidance

1.1. Introduction to the overarching information sharing ISA

The effective and timely sharing of information between agencies and organisations is essential to enable early intervention and preventative work for safeguarding and promoting welfare of those experiencing and at risk of abuse and harm and for wider public protection. For this reason, this Information Sharing Agreement (ISA) applies to all areas of adult and children's safeguarding e.g. including Prevent/Channel/Modern Slavery/Domestic Abuse etc.

This ISA sits beneath the overarching Information Sharing Protocol (ISP)/Partnership Agreement to which most of the Partners listed above are signatories.

There are other reasons for agencies to share information which are not covered by this agreement such as the obligation for agencies to share information with their regulators for the purpose of assurance.

It should be read in conjunction with the Leicester, Leicestershire & Rutland Safeguarding Procedures:

https://llrscb.proceduresonline.com/index.htm

https://www.llradultsafeguarding.co.uk

1.2. Purpose – Why do you need to share this information?

The purpose of this Information Sharing Agreement (ISA) is to facilitate the lawful sharing, use and security of personal, special categories of personal data and criminal offence data in order to safeguard adults and children who are at risk of abuse or neglect: when sharing information in response to managing safeguarding concerns and to facilitate the statutory functions of the Adult Safeguarding Boards and Childrens Safeguarding Partnerships.

1.3. Legal Basis – What law allows you to share this information?

Information must be shared lawfully. A public authority can only work within the legal framework which relates to your agency/organisation (Ultra vires rule).

1.4. Statutory gateways for information exchange

General Safeguarding Legislation

Care Act 2014 - S.6(1); S.42; S.45

Crime and Disorder Act 1998 – Section 115

Crime and Disorder (Prescribed Information) Regulations 2007. SI 1831

Criminal Justice Act 200

Domestic Violence, Victim & Witnesses Act 2004

Mental Capacity Act 2005

Police Act 1996

Police and Justice Act 2006

Protection from Harassment Act 1997

Safeguarding Vulnerable Groups Act 2006

Child Specific

Children Act 1989 S17(10); S27; S47; Part 1, Schedule 2, Para 1

Children Act 2004 – S10; S11; S14B; S17; S47

Guidance

Care and Support Statutory Guidance Oct 2014

Multi-Agency Public Protection Arrangements (MAPPA)

Safeguarding Children and Young People: The RCGP/NSPCC Safeguarding Children Toolkit for General Practice 2014

Working Together to Safeguard Children 2013, 2015 and 2018.

Keeping children safe in education (Statutory guidance for schools and colleges on safeguarding children and safer recruitment.

1.5 Compliance with Data Protection Legislation and Human Rights Act 1998 (HRA) and common law duty of confidence

The Data Protection Legislation[1] (Human Rights Act 1998 (HRA) and common law duty of confidence, do not in themselves provide a legal basis for disclosure of information. However, disclosure of personal data must satisfy their requirements.

Section 2 – Information Sharing:

Effective Sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision in order to keep children and young people, and vulnerable adults safe.

Practitioners should be proactive in sharing information as early as possible to help to identify, assess and respond to risks and concerns about the safety and welfare of children, young people and vulnerable adults; whether this is an emerging issue or whether they are already known to local authorities.

[1] 'Data Protection Legislation' means the Data Protection Act 2018, the Retained General Data Protection Regulation 2016/679 (UK GDPR), the Law Enforcement Directive 2016, the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable Laws relating to processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and protect those at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping an individual safe.

2.1 Information Sharing: Data Protection Law

The Data Protection Act 2018 and Retained General Data Protection Regulations (UK GDPR) do not prevent the sharing of information for the purposes of keeping children, young people and vulnerable adults safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children, young people and vulnerable adults.

To ensure effective safeguarding arrangements:

- All organisations and agencies should have arrangements in place that set out clearly the processes and principles for sharing information. The arrangements should cover how information will be shared with their own organisation/agency and other who may be involved in a child, young persons or vulnerable individuals' life.
- All practitioners must not assume that some else will pass on information that they think may be critical. If a practitioner has concerns about someone's welfare and considers that they are a child in need or vulnerable adult, or is likely to suffer from significant harm, then they should share the information with the local authority and/or the police. All practitioners should be particularly alert to the importance of sharing information when a child moves from one local authority into another, due to the risk that knowledge pertinent to keeping a child safe could be lost.
- Data protection law provides a number of lawful bases for sharing personal information. It is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child, young person or vulnerable adult provided that there is a lawful basis to process any personal information required. The legal bases that are most commonly appropriate for sharing information in these circumstances are 'legal obligation' or 'public task' which includes the performance of a task in the public interest or the exercise of official authority. Each legal basis under data protection law has different requirements[2]. In some circumstances it might be appropriate to seek consent to share information but it is important to note that data protection legislation sets a high standard for consent which is specific, time limited and can be withdrawn (in which case the information would need to be deleted).

Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for under the Data Protection Act 2018 and the UK GDPR. To share information effectively:

- All practitioners should be confident in the lawful bases and processing conditions under Data Protection legislation which allow them to store and share information including information that is considered sensitive, such as health data, known under data protection legislation as 'special category' personal data.

[2] Further ICO guidance on lawful bases to share information can be found at Appendix B

- Where practitioners need to share special category personal data, for example, where information obtained is sensitive and needs more protection, they should always consider and identify the lawful bases for doing so under Article 6 of GDPR, and in addition be able to meet ne of the specific conditions for processing under Article 9 of GDPR. In effect, Schedule 1 of the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information, including without consent (where in the circumstances consent cannot be given, it cannot be reasonably expected that a practitioner obtains consent or if to gain consent would place a child or vulnerable adult lacking capacity at risk). However, practitioners should be mindful that a data protection impact assessment (DPIA) for any type of processing which is likely to be high risk must be completed, and therefore aware of the risks of processing special category data. This is why information sharing agreements between organisations/agencies are supported by DPIAs therefore providing practitioners with confidence that risks associated with data sharing under the agreement have been considered.

Conditions for sensitive processing - Schedule 8 Section 35(5) of the Data Protection Act 2018 sets out the lawful grounds for processing of special category data for safeguarding of children and of individuals at risk – including without consent if the circumstances justify it –

(1) This condition is met if—

a. The processing is necessary for the purposes of:

   i. Protecting an individual from neglect or physical, mental or emotional harm; or

   ii. Protecting the physical, mental or emotional well-being of an individual.

b. The individual is:

   i. Aged under 18; or

   ii. Aged 18 or over and at risk.

Where there is a clear risk of significant harm to a child, or serious harm to adults the basis on which you can share information is clear. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, may be more difficult to judge. Practitioners should discuss with their line manager or designated safeguarding lead the need to share information when there are concerns about a child or young person. The information shared should be proportionate and a record should be kept of what has been shared, with whom and for what purpose and the reasoning behind it.

Myth-busting guide to information sharing

Sharing information enables practitioners and agencies to identify and provide appropriate services that safeguard and promote the welfare of adults and children. Below are common myths that may hinder effective information sharing.

Data protection legislation is a barrier to sharing information
No – the Data Protection Act 2018 and UK GDPR do not prohibit the collection and sharing of personal information, but rather provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them.

Consent is needed to share personal information
No – you **do not** need consent to share personal information. It is one way to comply with the data protection legislation but not the only way. The UK GDPR provides a number of bases for sharing personal information. It is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of an adult or child provided that there is a lawful basis to process any personal information required. The legal bases that may be appropriate for sharing data in these circumstances could be 'legal obligation', or 'public task' which includes the performance of a task in the public interest or the exercise of official authority. Each of the lawful bases under UK GDPR has different requirements.[15] It continues to be good practice to ensure transparency and to inform parent/ carers that you are sharing information for these purposes and seek to work cooperatively with them.

Personal information collected by one organisation/agency cannot be disclosed to another
No – this is not the case, unless the information is to be used for a purpose incompatible with the purpose for which it was originally collected. In the case of children in need, or children or vulnerable adults at risk of significant harm, or it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.[3]

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information
No – this is not the case. In addition to the Data Protection Act 2018 and UK GDPR, practitioners need to balance the common law duty of confidence and the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

IT Systems are often a barrier to effective information sharing
No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful for information sharing. IT systems are most valuable when practitioners use the shared data to make more informed decisions about how to support and safeguard a child.

2.2 Information Sharing: Confidentiality and Human Rights

In addition to the UK GDPR and Data Protection Act 2018, practitioners need to balance the common law duty of confidence, and the rights within the Human Rights Act 1998,

[3] Practitioners looking to share information should consider which processing condition in the Data Protection Act 2018 is most appropriate for use in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

against the effect on children or individuals at risk, if they do not share the information through the application of a Public Interest test.

If information collection and sharing is to take place with the consent of the individuals involved this should be considered as a point of transparency and only where there is no risk to them or another individual, as there is likely to be a legal obligation or public interest test justifying the disclosure of information.

Providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998. In the context of safeguarding, where the individuals' welfare is paramount, it is possible that the common law duty of confidentiality can be overcome. Practitioners must consider this on a case-by-case basis. As is the case for all information processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared.

2.3 Information sharing with Non-statutory agencies e.g. charities

There are a number of charitable organisations that offer support and services. Such organisations are not created under statute and therefore do not have statutory powers; nevertheless, they are often able to offer help and assistance in the form of counselling, advice, support and guidance as well as referring individuals to other organisations and charities within their network.

The minimum amount of information should be disclosed to achieve the objective. For example, when referring an adult victim of abuse, it may not be appropriate to disclose the injuries sustained, but it may be appropriate for the safety of agencies involved to disclose relevant information about the perpetrator. When referring a perpetrator, then, the relevant information about the victim may need to be disclosed. It may be necessary to provide relevant information regarding the risk assessment – for example, safe means and times of contact. (Disclosure must be considered on a case–by-case basis, proportionate to the situation and the decision making recorded). Both partners need to consider the Accountability principle and ensure that they record what has been shared, the purpose for the sharing, when and with whom.

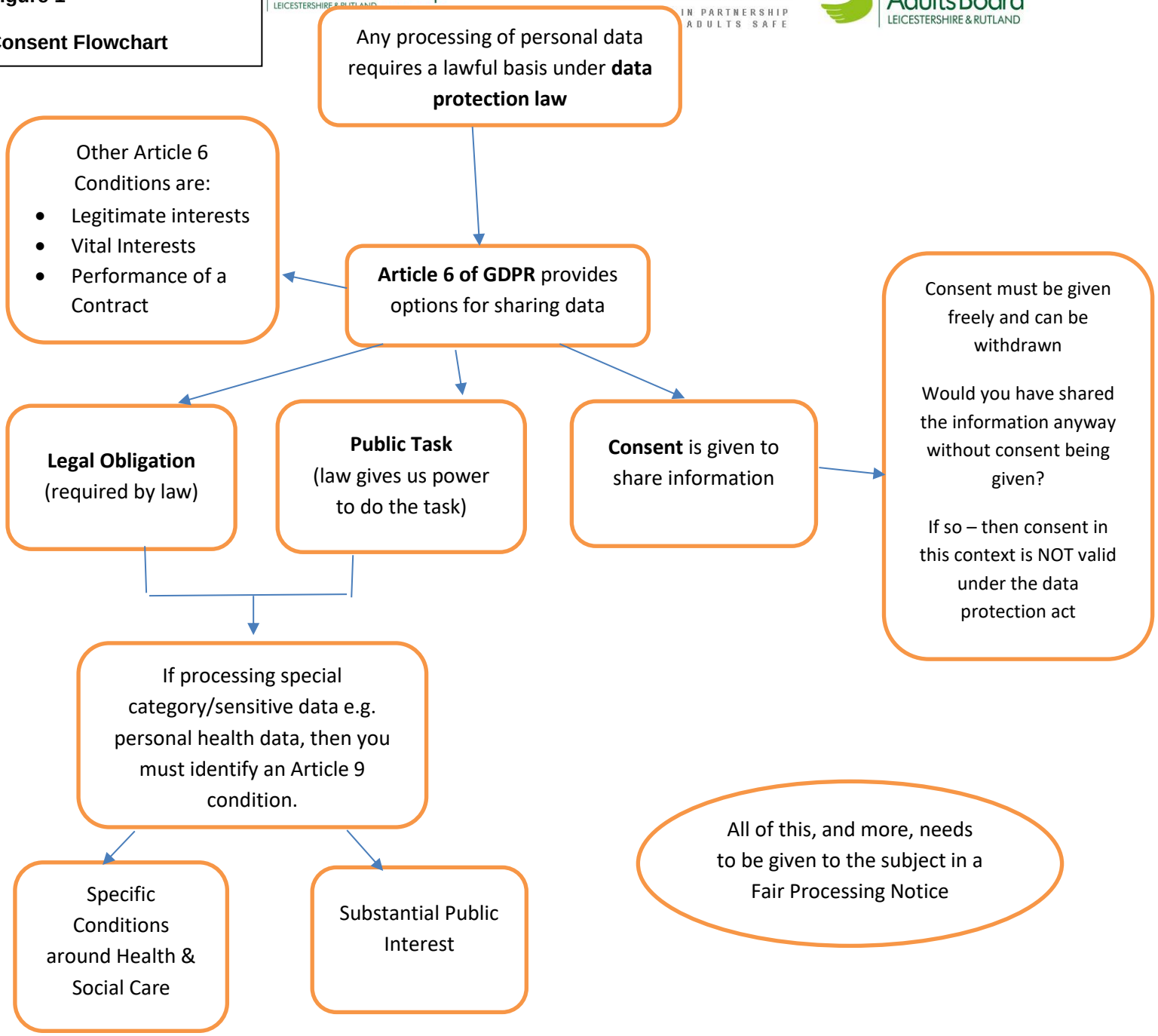
2.4 People lacking capacity

When sharing information in respect of adults who lack the capacity to provide any required agreement to support (reference to 2.3), information should only be shared when it is permitted by relevant legislation and if considered to be in the person's best interests.

Additionally, where a person lacks mental capacity to decide about their own personal information, the Mental Capacity Act 2005 Code of Practice states that certain other people may be able to request access to that information. This would be somebody with a lasting power of attorney, an enduring power of attorney or who is a deputy appointed by the Court of Protection. Again, the decision making should be recorded.

Figure 1

Consent Flowchart



COMMON LAW DUTY

(this runs alongside the Data Protection Act & GDPR)

When dealing with health and social care data, and there is a **duty of confidence** inferred in the relationship e.g. social worker to service user, police to a victim of crime, then the **Common Law Duty** applies.

Service users need to be given the opportunity to /agree to the process. This is different to a lawful basis under Data Protection that allows their data to be shared.

Consenting/agreeing to the process means the worker must be clear on where their data will be shared and why. The service user must also be given the opportunity to agree or object to this.

As a worker you need to ensure that the above is explained to service users when processing personal data and a duty of confidence is owed.

Children and Young People

For children under 16 years of age, the Mental Capacity Act does not apply. Instead, a child needs to be assessed whether they have enough understanding to make up their own mind about the benefits and risks – this is termed Gillick competence. Generally, in these circumstances agreement will be sought from their parents.

Once children reach the age of 16, they are presumed in law to be competent. However, if they do not have the capacity to agree, the Mental Capacity Act applies.

2.5 Child Death Reviews

Statutory Requirements

The Child Death Review arrangements in Leicester, Leicestershire & Rutland (LLR) are carried out by the Child Death Overview Panel (CDOP) to review the deaths of children on behalf of the Department of Health under the requirements of the Statutory & Operational Guidance 2018.

When a child dies, in any circumstances, it is important for parents and families to understand what has happened and whether there are any lessons to be learned.

The responsibility for ensuring child death reviews are carried out is held by 'child death review partners.'

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

Child death review partners for two or more local authority areas may combine and agree that their areas be treated as a single area for the purpose of undertaking child death reviews.

Child death review partners must make arrangements for the analysis of information from all deaths reviewed.

The purpose of a review and/or analysis is to identify any matters relating to the death, or deaths, that are relevant to the welfare of children in the area or to public health and safety, and to consider whether action should be taken in relation to any matters identified. If child death review partners find action should be taken by a person or organisation, they must inform them. In addition, child death review partners:

- must, at such times as they consider appropriate, prepare and publish reports on:

- what they have done as a result of the child death review arrangements in their area, and

- how effective the arrangements have been in practice; • may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process - the person or organisation must comply with the request under section 10 & 11 of

the Children Act 2004, and if they do not, the child death review partners may take legal action to seek enforcement: and

• may make payments directly towards expenditure incurred in connection with arrangements made for child death reviews or analysis of information about deaths reviewed, or by contributing to a fund out of which payments may be made; and may provide staff, goods, services, accommodation or other resources to any person for purposes connected with the child death review or analysis process.

2.5.1 Child Death Overview Panel (CDOP)

In Leicester, Leicestershire and Rutland (LLR) there is one panel that oversees all cases that require a review. The Child Death Overview Panel meets regularly to complete a multi-agency evaluation of all child deaths in the area.

The Child Death Review manager and panel, on behalf of the Child Death Review Partners (Local Authorities and Integrated Care Boards), oversees notification of deaths. Data submissions are sent to the National Child Mortality Database (NCMD) for all cases, and then in the annual report to the Child Death Review Partners.

The panel, which, at the time of publication is currently chaired by a Public Health Consultant, aims to identify local lessons and issues of concern, and, where appropriate, to advocate the need for changes in policy, practices and public awareness. The aim is to promote child health and safety and help prevent future child deaths.

More details regarding the core purpose and key functions can be found here: https://llrscb.proceduresonline.com/p_child_death_review.html

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859302/child-death-review-statutory-and-operational-guidance-england.pdf

Templates to support the CDOP process can be found here:- https://www.gov.uk/government/publications/child-death-reviews-forms-for-reporting-child-deaths

Section 3 – Information Sharing: Ownership and Security

3.1. What Information does each signatory need to share?

This Information Sharing Agreement has been produced to include a number of both operational and review purposes.

These include:

- Information that indicates reasonable cause to suspect that an adult or Child/young person is experiencing or at risk of abuse or neglect
- For the purposes of information sharing in response to protecting adults and children/young people at risk of neglect and abuse
- For the purposes of the Leicester and Leicestershire & Rutland Local Safeguarding Adults and Children's Boards/Partnerships when commissioned by the Community

Safety Partnership to conduct Safeguarding Adults Reviews (SARs), Local Child Safeguarding Practice Review., Domestic Homicide Reviews (DHRs) and other learning review and audit processes. Reference the previous information on SARs

The following are the types of data that may be proportionate, relevant and necessary to share between partners for the purposes of safeguarding adults, but this must be decided on a case–by-case basis. It is important to remember that there must be a legitimate reason for obtaining each piece of information and the legality of continuing to hold the information such as retention, as this amounts to processing and processing requires justification.

Example of the data required – case specific/relevant
Name(s) and Alias'
Dates of Birth and Dates of Death (if applicable)
Current Address and Previous Addresses
Contact information and Next of Kin
Family Information and dependants
Information on contacts with service/team
Outcomes of contacts
Names of key workers/staff involved
Alleged perpetrator and their relationship to the victim
Health Information (GP/Health Workers involved)
Photos of injuries sustained
Care Plans and associated documentation
History of offences
Disclosure and Barring
Risk flags on systems (warning markers)
Any other relevant information

A thorough process to support the reason for requesting any personal information ensures that information is only requested where there is a justifiable need, rather than "nice to know".

When a professional has made the decision to share information s/he must –

- Ensure information shared is necessary, relevant and proportionate for the purpose for which it is being shared
- Understand the limits of any consent given, especially if the information has been provided by a third party
- Distinguish fact from opinion
- Check that the information is accurate and up-to-date
- Share the information only with the person or people who need to know
- Share the information in a secure way
- Establish whether the recipient intends to pass it on to other people, and ensure the recipient understands the limits of any consent that has been given (where appropriate)
- Ensure that the person to which the information relates (or the person who provided the information) is informed that you are sharing information where it is safe to do so
- To record the decision, how it was made, what information was shared and with whom.

3.2. Who will own the information?

The Data Controller of the agency/organisation or Chief Constable, in the case of the Police, who originally holds the personal information is the Data Controller. Once that information is shared with another partner to this ISA, the Data Controller of the agency/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.

3.3. How are you going to keep information accurate?

It is the responsibility of each partner agency to ensure as far as possible the information they supply is accurate. Care should be taken when checking the accuracy of the information to be shared and the details of the person or agency the information will be shared with, and any inaccuracies are corrected and providence provided.

3.4. Security of Information

The information required under this ISA is personal and sensitive personal information and should be considered to be “Official-Sensitive” under the Government Classification Scheme when applying the security requirements in Appendix A

If telephone calls are used to share information, care needs to be taken and checks undertaken, to ensure that information is being disclosed to the authorised person in advance of any sharing.

The most secure electronic method available and agreed within your own agency and between agencies should be used.

3.5. How long will the information be kept?

Each agency/organisation which has received information referred to in this agreement will have their own Retention and Disposal Policy which should state how long they will keep different types of information. Therefore, each partner will retain the information for as long

as necessary to achieve the purpose and in accordance with the Retention and Disposal Policy.

Please refer to individual agencies policies for details.

3.6. How will we keep information secure?

Each Controller has a legal duty under Article 5 (1) (f) of the UK GDPR and under DPA 2018, to keep the personal information they hold secure from any unauthorised, unlawful processing and from accidental loss, or destruction of, or damage to personal information.

Personal information will be held securely within each agency's/organisation's electronic file structure in accordance with their own organisational security measures.

3.7. What if we want to use the information for something else?

If any agency/organisation wishes to use the information which they have been given under this agreement, for any other purpose other than that in Section 2 above, they must first ask the agency/organisation which provided the information for their written agreement to ensure compliance with the Data Protection legislation, unless the partner has a statutory obligation, or the individual is at risk/crime prevention

3.8. What do we do if information is lost, disclosed, misused, etc. (data security breach)?

If any information which is shared under this agreement is lost, stolen or disclosed to someone who should not have seen it, this is not only a breach of confidentiality but is likely to be a breach of the Data Protection legislation. If the information is deliberately accessed and/or disclosed by someone who is not entitled to see or use it, this person may have committed a criminal offence under the Data Protection Legislation and/or the Computer Misuse Act 1990.

Any breaches of this Agreement must be reported to the Controller that provided the information immediately so that they can risk assess what has happened. An investigation may have to be undertaken by the Police to determine whether any criminal investigations are required. If the breach has serious implications, the Information Commissioner must be notified within 72 hours. It is the responsibility of the controller, where the breach occurred, to inform the ICO. If an investigation is undertaken by the Police or the ICO, evidence including audit trails and printouts may be recovered.

All partners involved in the breach will investigate and record the breach and the outcome of the breach will be circulated to the partners involved in the breach, to ensure procedures around informing the data subject and ICO are met. The agency/organisation where the breach occurred may need to do an internal investigation and this may lead to disciplinary action or identifying processes which need to be changed.

Each agency/organisation should provide contact details of the post in their agency/organisation who should be informed if an information breach occurs in the table below.

Agency/Organisation	Post	Email	Telephone

3.9. How will you check if your colleagues are complying with this agreement and if it is still current?

The Adult Safeguarding Boards and The Safeguarding Children Partnerships, on behalf of the agencies who are party to this agreement, will review this agreement within 1 year of commencement of this ISA, and then subsequent 2 years.

As part of the case file audits and case review audits undertaken as part of the Assurance Framework, the following aspects will be reviewed:

- Information shared appropriately and timely
- Breaches are investigated and analysed in order that the agreement is reviewed
- Potential surveys
- Safeguarding Assurance Cycle Process

3.10. What happens if there is a major security breach?

Any agency/organisation can suspend this ISA for 30 days if security has been seriously breached and all signatories informed immediately. This should be in writing and provide evidence of what went wrong. A representative from each agency/organisation should meet as soon as possible (no longer than 14 days) to carry out a Risk Assessment and Resolution meeting.

3.11. Indemnity

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

In the case of Multi-agency meetings, there is the potential for a scenario where organisations are Joint Controllers. In these circumstances indemnity clauses and confidentiality requirements will be set out by the administration of the meeting.

3.12. What do we do if the Data Subject asks for information which we receive under this ISA?

3.12.1. Data Protection Legislation

An agency/organisation may receive an Information Rights Request under the Data Protection legislation by the data subject. In Leicester, Leicestershire and Rutland, it has been agreed that when an agency/organisation receives such a request, which has been shared under this ISA, the agency/organisation that receives the request will consult with the agency/organisation which provided the information and consider their views as part of its decision making process in respect of how to respond in terms of any disclosures/objections/rectification or erasure.

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

All recorded information held by public authorities is subject to the provisions of FOIA and EIR. An agency/organisation may receive a request under the FOIA or EIR. It has been agreed that when an agency/organisation receives a request for information which has been shared under this ISA, the agency/organisation which receives the request will consult

with the agency/organisation which provided the information and consider their views as part of its decision-making process in respect of how to respond to the request.

Nothing in this section shall prevent any partner agency/organisation from exercising its obligations and responsibilities under the FOIA or the EIR as they see fit.

3.13. Who are the Responsible People in each agency/organisation?

Information sharing activity should be reviewed and approved by the agency's/organisation's legal/information security staff/information management team. Each agency/organisation should give details of the post which is responsible on a day to day basis for monitoring compliance with this ISA.

3.14. Who are the Appropriate Signatories in each agency/organisation?

Each agency/organisation should identify who is the most appropriate post holder within their agency to sign the ISA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their agency/organisation to the agreement. Each agency/organisation must bear in mind this person will be making the commitment on behalf of the agency/organisation that the conditions in this ISA will be complied with.

Each agency/organisation who is a signatory to this ISA will be asked to complete the table below which will identify the appropriate post holder to sign this agreement on behalf of their agency/organisation. In addition, the agency/organisation will be asked to identify the post which is responsible on a day-to-day basis for monitoring compliance with this ISA.

Agency/Organisation:	
Person signing this Information Sharing Agreement	
Name:	
Role:	
Signature:	
Date:	
Responsible Person	
Post:	Director of Adult Services and Health
Address:	Rutland County Council Catmose Oakham Rutland LE15 6HP
Tel:	01572 758442
Email:	jmorley@rutland.gov.uk

APPENDIX A - 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 removable 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. Each Partner shall ensure that its officers/staff, authorised contractors and authorised representatives:

- Do not leave their workstation/PC signed on when it is not in use

- Minimise access to information and do not allow others to view the information displayed on their screens or in printouts that they are not entitled to view
- Lock away disks, tapes or printouts when not in use
- Exercise caution in what is sent via email and to whom it is sent. Emails containing personal information should be sent by secure email or if it has to be sent 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 UK GDPR or Data Protection Act 2018 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.

Sharing & Destruction Methods	**Security Requirements**
Agencies/Organisation Data Network (e.g. internal email)	Use of secure networks where available. If not, recommend password protecting attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title or sensitive personal data in body of email. Recommend turning off autofill of address field.
Email between partners	Password protecting attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title or sensitive personal data in body of email. To/from Police: restricted or sensitive personal data only to emails using secure email conventions. To/From NHS: secure transfer or other arrangement as agreed with health partners.

Laptops, removable media, USB, etc.	Must be owned by the employer and encrypted. No personal information from any of the agencies/organisations in this ISA is to be loaded to personally owned removable media.
Electronic storage of information	Has the application where it will be stored been pen tested? In other words, could someone hack into it? Check with your IT department. How will access to the information be restricted? Please say how this will be done Is there an audit trail which will show who has accessed a record?
Vetting/clearance of staff	Have the staff who will receive and access the information been vetted?
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
Fax	Note faxes are legacy technology and are NOT to be used unless there is no alternative. If no alternative, check recipient has a safe haven fax procedure in place. This should include a recipient being on hand to receive. Send cover sheet first and wait for confirmation before sending.
Storage of papers	Protected by one barrier: e.g. a locked container within a secure building/room. Locked filing cabinet for storage if home working.
Disposal of papers	Use secure waste sacks if agency/organisation has system in place and make sure they are secure when left unattended or collected for destruction. Shred personal and sensitive personal information
Disposal of magnetic media	All types of discs and other storage devices – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction.
Movement within agency/ organisation via internal mail	In a sealed envelope with protective marking shown.
Movement between partner agencies	By post or courier in a sealed envelope. Do not show protective marking on the envelope.

Movement between workplace and home/mobile office	On encrypted memory stick or lockable briefcase provided other security measures have been put in place i.e. if travelling by car the brief case is placed in the boot away from the public eye or is locked away in filing cabinet for storage if home working.

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

Each Controller must apply appropriate security measures in compliance with the Government Security Classifications 2014 or equivalent and commensurate with the requirements of principle 6 of the Retained General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to any Information from the Disclosing Party subject to such principle. This states that: "information will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"). The Information is classified as "Official-Sensitive" by the Disclosing Party under the Government Security Classifications 2014[1] and these, especially the standard control measures at paragraph 13-14, are recommended as good practice to the Receiving Party and indicate the standard of security which is expected to be applied to Information received under this Agreement.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

APPENDIX B – Legal Table

Legislation relevant at the time of the review of this agreement

Lawful Information Sharing	Organisation(s)
Personal Data – UK GDPR 6(1)(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; 6(1)(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller. Additional condition is required under Art 6(3) UK GDPR - **Personal data - DPA 2018** Part 2, Chapter 2, Section 8(c) the exercise of a function conferred on a person by an enactment or rule of law.	All Partners
Special Categories of Personal Data – UK GDPR 9(2)(g) processing is necessary for reasons of **substantial public interest**, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. **Special Categories of Personal Data – DPA 2018** Additional conditions under DPA 2018 – SCH: 1 PART 2 Statutory etc. and government purposes 6 (1) This condition is met if the processing— (a) is necessary for a purpose listed in sub-paragraph (2), and (b) is necessary for reasons of substantial public interest. 6 (2) Those purposes are— (a) the exercise of a function conferred on a person by an enactment or rule of law; (b) the exercise of a function of the Crown, a Minister of the Crown or a government department. Preventing or detecting unlawful acts 10 (1) This condition is met if the processing— (a) is necessary for the purposes of the prevention or detection of an	All Partners

unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest. Safeguarding of children and of individuals at risk 18 (1) This condition is met if— (a) the processing is necessary for the purposes of— (i) protecting an individual from neglect or physical, mental or emotional harm, or (ii) protecting the physical, mental or emotional well-being of an individual, (b) the individual is— (i) aged under 18, or (ii) aged 18 or over and at risk, (c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) the processing is necessary for reasons of substantial public interest. Safeguarding of economic well-being of certain individuals 19 (1) This condition is met if the processing— (a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over, (b) is of data concerning health, (c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) is necessary for reasons of substantial public interest. NHS England and NHS Improvement Midlands (NHSEI) usually process special category data under Article 9(2)(h) of UK GDPR - processing necessary for health or social care.	
Criminal Offence Data – UK GDPR Article 10 (UK GDPR) - Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. **Criminal Offence Data – DPA 2018**	All Partners

Part 2, Chapter 2, Section 10(5) - The processing meets the requirement in Article 10 of the UK GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1. **Schedule 1:** Health or social care purposes Public Health Administration of justice and parliamentary purposes Preventing or detecting unlawful acts Preventing fraud Safeguarding of children and individuals at risk Safeguarding of economic well-being of certain individuals Consent Protecting individual's vital interests Personal data in the public domain Judicial acts Administration of accounts used in the commission of indecency offences involving children Extension of conditions in Part 2 of this Schedule referring to substantial public interest.	
Crime & Disorder Act 1998 115(1) Any person who, apart from this subsection, would not have power to disclose information – (a) to a relevant authority; or (b) to a person acting on behalf of such an authority, shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act only. **S17 (1)** Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in its area.	Police Service Police Authority Health Authority Fire Services Authority Local Authority Probation Trust Local Probation Board in England and Wales A person registered under section 1 of the Housing Act 1996 as a social landlord.
Common Law is law developed by custom and general agreement which is not enshrined in statute but never the less gives the police a duty to investigate crimes.	Police Service
The Police Act 1996	Police Service

The Police Act (1996) gives a Constable certain powers. The police have a general common law power to disclose information for policing purposes, usually for one or more of the following purposes: • prevention and detection of crime, • apprehension and prosecution of offenders, • protection of life and property and assisting the public. This allows the disclosure of identifiable information on a case-by-case basis for these purposes subject to appropriate safeguards.	
The Police and Justice Act 2006	
Safeguarding Vulnerable Groups Act 2006	
Mental Capacity Act 2005 Legislation that complements the framework relating to persons who lack capacity, particularly where decision-making needs to be made on their behalf, both where mental capacity has been lost and where the incapacitating condition has been present since birth. Section 4B Deprivation of liberty necessary for life-sustaining treatment etc.	Local Authority
Code of Practice to Mental Capacity Act 2005 Code of Practice. Chapter 2 Guiding principles. Chapter 16 what rules govern access to information about a person who lacks capacity. 16.19-16.23 refers	Local Authority

Mental Health Crisis Care Concordat 2014 https://www.gov.uk/government/publications/mental-health-crisis-care-agreement This agreement supports the ongoing directive on crisis care by allowing the effective and efficient flow of information to protect those who are vulnerable.	Local Authority
Criminal Justice Act 2003 The Act imposes a duty on police authorities and others to make arrangements to assess and manage risks posed by violent and sexual offenders. Section 325 (1) Of this Act details the arrangements for assessing risk posed by different offenders. The "responsible authority" in relation to any area, means the chief officer of police, the local probation board and the Minister of the Crown exercising functions in relation to prisons, acting jointly. (2) The responsible authority must establish arrangements for the purpose of assessing and managing the risks posed in that area by: (a) relevant sexual and violent offenders; and	**Responsible Authority:** Police Local Probation Board **Persons in s6** Youth Offending Team Ministers of the Crown, Local education authority Local Housing Authority.

(b) other persons who by reason of offences committed by them are considered by the responsible authority to be persons who may cause serious harm to the public (this includes children). (3) In establishing those arrangements, the responsible authority must act in co-operation with the persons specified in subsection (6); (4) Co-operation under subsection (3) **may** include the exchange of information.	Social Services Registered Social Landlords Health Authority or Strategic Health Authority Primary Care Trust, Local Health Board or NHS Trust.
Domestic Violence, Victim & Witnesses Act 2004 The Act gives specific powers and guidance for those dealing with offenders in breach of restraining orders or non-molestation orders.	Local Authority Police Service Social services
Domestic Violence, Victim & Witnesses Act 2004 Section 9 of the Act gives specific powers to compile the Domestic Homicide Review (DHR) and to provide a copy to the Board when required to do so. (s9 came in in April 2011)	Social Services Local Authority Police Service Probation Board Strategic Health Authorities
Multi-Agency Public Protection Arrangements (MAPPA) MAPPA Guidance: MAPPA is co-ordinated by the Public Protection Unit within the National Offender Management Service. Forms the basis of public protection, including protection to children, and which operate on a multi-agency partnership basis throughout England and Wales. **The Criminal Justice and Court Services Act 2000** This Act established formal arrangements for the supervision of people in the community, which required police and probation authorities to involve health in the arrangements. Subsequently, through the Criminal Justice Act 2003 this became a "duty to cooperate" on health and other agencies. Strictly speaking, this is a duty to cooperate with a process rather than to divulge information about a particular individual, although such disclosure may be required in some cases. The latter is usually, and correctly, subject to detailed local agreements.	Police Service Health Authority Fire Services Authority Local Authority Probation Prisons
The Protection from Harassment Act 1997 The Act gives specific powers and guidance in respect of harassment and putting or seeking to put another in fear of violence. It also includes breaches of civil injunctions or restraining orders.	Local Authority Police Probation
Care Act 2014 This Act provides information sharing powers between the relevant parties in order to protect the adult. Section 6 (1) A local authority must co-operate with each of its relevant partners, and each relevant partner must co-operate with the authority, Section 42. Enquiry by local authority.	Local Authority **Relevant Authorities:** NHS Police Probation

This section applies where a local authority has reasonable cause to suspect that an adult in its area has needs is at risk or requires support Section 45. Supply of information. Information may be used by the SAB, or other person to whom it is supplied only for enabling or assisting the SAB to exercise its functions. Care and Support Statutory Guidance, Chapter 14 covers Safeguarding	Safeguarding Adults Board Prisons NHS Integrated Care Board
Children Act 1989 Children Act 2004 Working Together to Safeguard Children 2018 Chapter 2 includes a section on Information Sharing Working Together: transitional guidance Statutory guidance to support Safeguarding Children Partnership (SCP), the new safeguarding and child death review partners, and the new Child Safeguarding Practice Review Panel in the transition from SCPs and serious case reviews (SCRs) to a new system of multi-agency arrangements and local and national child safeguarding practice reviews. Keeping children safe in education.	
Crime and Disorder (Prescribed Information) Regulations 2007	
Safeguarding Children and Young People: The RCGP/NSPCC Safeguarding Children Toolkit for General practice	
Royal College of General Practitioners Child Safeguarding Toolkit	
Female Genital Mutilation (FGM) FGM is a form of child abuse and violence against women and girls, and therefore should be dealt with as part of existing child and adult protection structures, policies and procedures. Further details regarding FGM can be found in the Government Multi-Agency Practice Guidelines for FGM.	
Child Sexual Exploitation Information may be shared under this agreement for the following purposes:	

• To facilitate best practice to provide a more integrated and coordinated approach to identified victims of Child Sexual Exploitation • To inform multi agency actions to prevent abuse occurring, disrupt perpetrator activity and secure evidence to support prosecutions, this may involve sharing intelligence gathered through the course of routine work, for example if a cohort of young people or vulnerable adults are found to have similar sexually transmitted infections or professionals involved are concerned about relationships in an area that could be potentially coercive. In adopting this partnership approach partners will work together to identify, support and safeguard children and young people and vulnerable adults who are vulnerable to sexual exploitation from those who are intent on abusing them. Acknowledgement: Barnsley Safeguarding Children Board - 21 March 2014	
Private Fostering LLR Procedures 2.9 Children Living Away from Home A private fostering arrangement is essentially one that is made without the direct involvement of a Local Authority for the care of a child under the age of 16 (under 18 if disabled) by someone other than a parent or close relative for 28 days or more. A close relative is defined as "a grandparent, brother, sister, uncle or aunt (whether of the full blood or half blood or by marriage or civil partnership) or step-parent. Becoming aware that a child is being privately fostered requires vigilance by practitioners. Teachers, health (particularly GPs and Health Visitors) and other professionals should notify the appropriate Duty Team of a private fostering arrangement that comes to their attention, where they are not satisfied that the arrangement has been or will be notified. The family are to be advised to notify the local authority about the arrangement.	
Early Help/Support The purpose of early help and prevention is to improve outcomes for children and young people at all stages of their development; from pre-birth, through the early years stage, throughout their school careers and on into their transition to adulthood. Difficulties may emerge at any point throughout childhood and adolescence.	
Counter Terrorism and Security Act 2015 **Section 36 – Assessment and Support local panels**	

This sections consists of information that can be used by local panels to plan their assessment and support packages. Each local authority must ensure that a panel of persons is in place for its area (Channel) The functions of a panel referred to in subsection are— (a)to prepare a plan in respect of identified individuals who the panel considers should be offered support for the purpose of reducing their vulnerability to being drawn into terrorism; (b)if the necessary consent is given, to make arrangements for support to be provided to those individuals in accordance with their support plan; (c)to keep under review the giving of support to an identified individual under a support plan; (d)to revise a support plan, or withdraw support under a plan, if at any time the panel considers it appropriate; (e)to carry out further assessments, after such periods as the panel considers appropriate, of an individual's vulnerability to being drawn into terrorism in cases where— (i)the necessary consent is refused or withdrawn to the giving of support under a support plan, or (ii)the panel has determined that support under a plan should be withdrawn; (f)to prepare a further support plan in such cases if the panel considers it appropriate. (5)A support plan must include the following information— (a)how, when and by whom a request for the necessary consent is to be made; (b)the nature of the support to be provided to the identified individual; (c)the persons who are to be responsible for providing it; (d)how and when such support is to be provided. (6)Where in the carrying out of its functions under this section a panel determines that support should not be given to an individual under a support plan, the panel— (a)must consider whether the individual ought to be referred to a provider of any health or social care services, and	

(b)if so, must make such arrangements as the panel considers appropriate for the purpose of referring the individual.

(7)In exercising its functions under this section a panel must have regard to any guidance given by the Secretary of State about the exercise of those functions.

Section 38

Co-operation

The partners of a panel must, so far as appropriate and reasonably practicable, act in co-operation with—

(a)the panel in the carrying out of its functions;

(b)the police in the carrying out of their functions in connection with section 36 (see above).

(3)The duty of a partner of a panel to act in co-operation with the panel—

(a)includes the giving of information (subject to subsection (4)

(b)extends only so far as the co-operation is compatible with the exercise of the partner's functions under any other enactment or rule of law.

(4)Nothing in this section requires or authorises the making of—

(a)a disclosure that would contravene the data protection legislation;

(b)a disclosure of any sensitive information.

(4A)“The data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).

(5)“Sensitive information” means information—

(a)held by an intelligence service,

(b)obtained (directly or indirectly) from, or held on behalf of, an intelligence service,

(c)derived in whole or part from information obtained (directly or indirectly) from, or held on behalf of, an intelligence service, or

(d)relating to an intelligence service.

APPENDIX C - Security of Shared Information for National Probation Service

The Information Recipient agrees to process all the shared information in accordance with the following security requirements:
a. The recipient is required to have an CJSM and/or an approved email

b. access to the shared information, any copies made of the shared information and the information contained in them is limited solely to the persons specified in this ISA;

c. access to the shared information is minimised to the smallest pool of accessible records possible;

d. the confidentiality of the shared information will be preserved in outputs and publications, as detailed. The shared information will not be matched or linked with any other Information or information sources. No duplication of the Shared Information may take place or copies of the Shared Information be made other than as agreed in the purpose of the ISA.;

e. shared Information will only be accessed by devices or services that are themselves subject to restricted access.

f. Access to cloud-hosted or on-premise devices or services that can access the shared information will only be through mechanisms that comply with HMG Security Policy Framework such as suitability strong passwords and multi-factor authentication https://www.gov.uk/government/publications/security-policy-framework

g. the means of access to the shared information (such as passwords or passphrases) will be kept secure and not disclosed to any person or service, under any circumstances other than those specified in this ISA;

h. hard copies and backups of shared information will be stored in a secure, access restricted filing cabinet or shared folder;

i. shared information will not be accessed at a location outside the UK;

j. shared information should be held and accessed on paper or ICT systems on secure premises;

k. whenever possible, data should be protected by Transport Layer Security when in transit i.e. communicated over the open internet and encrypted at rest i.e. when its resident on another domain."

l. the Information is backed up in case of corruption.

m. technical and organisational controls and processes for system, network and security capabilities and components are tested regularly to maintain and demonstrate the continuing correctness of their operation and correct functioning.

n. logs of processing operations as set out in section 62 of the DPA will be kept for all Information processing in this information share for law enforcement purposes (as defined by section 31 of the DPA

National Probation Service reserves the right to conduct an on-site audit of the Information Recipient's confidentiality and security procedures and practices, or to require a report of such an audit by an independent assessor.