Berkshire Local Safeguarding Children Boards

Data and Information Sharing Agreement for Agencies Working with Children and Young People

June2016

CONTENTS

This document is broken down into three separate parts:

1. Part 1 is the overarching Information Sharing Agreement which is approved by partners of the six Berkshire Local Safeguarding Children Boards.
2. Part 2 is the template for the development of a local Information Sharing Agreement to support the delivery of multi-agency work at an operational level, or to support specific multi-agency service delivery activity.
3. Part 3 consists of annex documents with additional information for practitioners.

PART 1 – INFORMATION SHARING AGREEMENT

1. INTRODUCTION

Information sharing within Berkshire services for children, young people and families

Sharing information is key to the goal of delivering better, more efficient public services that are coordinated around the needs of the individual, families and communities. It is essential to enable early intervention and preventative work, for safeguarding and promoting welfare of children and young people and for wider public protection. Information sharing is a vital element of improving outcomes for all.

Each time a Serious Case Review is published there is always a shortfall in the practice and process of sharing information between agencies which have led to failures in protecting the child. Continuous recommendations are made that systems are put in place in every local authority area to ensure that information about children and young people can be shared appropriately within and between agencies.

This Agreement provides a framework for agencies to share information about children, young people and families who are receiving services or for whom they have a concern and to support information sharing to develop services to support children, young people and families. It sets out the principles for sharing information and gives the legal context in which we share information.

If there are concerns that a child or an adult may be at risk of significant harm, then it is your duty to follow the relevant procedures without delay. Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Principles for Information Sharing – Seven Golden Rules from HM Government

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You should go **ahead** and share information without consent if, in your judgement, that lack of consent can be overridden in the public interest, or where a child is at risk of significant harm. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the **information** you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Key Points on Information Sharing

1	You must explain to children, young people and families at the onset, openly and honestly, what and how information will, or could be shared and why, and seek their agreement. *The exception to this is where to do so would put that child, young person or others at risk of significant harm or an adult at risk of significant harm, or if it would undermine the prevention, detection or prosecution of a serious crime, including where seeking consent might lead to interference with any potential investigation.*
2	You must always consider the safety and welfare of a child or young person when making decisions on whether to share information about them. Where there is concern that the child may be suffering or is at risk of suffering significant harm, the child's safety and welfare must be the overriding consideration.
3	You should, where possible, respect the wishes of children, young people or families who do not consent to share confidential information. You may still share information if, in your judgement based on the facts of the case, there is sufficient need to override that lack of consent.
4	You should seek advice where you are in doubt, especially where your doubt relates to a concern about possible significant harm to a child or serious harm to others.
5	You should ensure that the information you share is relevant, accurate and up to date, necessary for the purpose for which you are sharing it, shared only with those people who need to see it and shared securely.
6	You should always record the reasons for the decision, whether it is to share information or not.

Good information sharing is based on good recording practice. Records should be accurate, relevant, kept up to date, and kept for no longer than is necessary for their purpose. An audit trail of requests made and disclosures given will provide a record of events if required in the case of investigations or local inspections

Sharing information to support children

When there are child protection concerns consent is desirable but not necessary. The information needs to be proportionate.

Please see a link to the information sharing agreement for Multi-Agency Safeguarding Hubs which have been developed by individual local authorities to support effective application of Threshold Guidance.

Reading MASH ISA link…….(to be inserted)

Wokingham MASH ISA link ……..(to inserted)

There is an increasing emphasis on integrated working across children's services so that support for children, young people and families is provided in response to their needs. The aim is to deliver more effective intervention at an earlier stage to prevent problems escalating and to increase the chances of a child or young person achieving positive outcomes.

Whether the integrated working is across existing services or through specific multi-agency structures, success depends on effective partnership working between universal services (such as education and primary health care) and targeted and specialist services for those children, young people and families at risk of poor outcomes.

Preventative services working in this way will be more effective in identifying concerns about significant harm, for example, as a result of abuse or neglect. However, in most situations children, young people and family members will require additional services in relation to education, health, behaviour, parenting or family support, rather than intervention to protect the child or young person from harm or to prevent or detect serious crime.

Effective preventative services of this type will usually require active processes for identifying children and young people at risk of poor outcomes, and passing information to those delivering targeted support. Practitioners sometimes express concern about how this can be done lawfully.

Statutory guidance **Working Together to Safeguard Children (2015)** states that effective sharing of information is essential for effective identification, assessment and service provision. It also states that early sharing of information is the key to providing effective early help where there are emerging problems.

A generic information sharing agreement specifically for Child Sexual Exploitation operational groups is available for use via this link: ……(to be inserted)

Specific information sharing guidance has been developed by health partners – Female Genital Mutilation and Child Sexual Exploitation. Link to RBH CSE doc and FGM protocol ……(to be inserted)

There are clear statutory requirements to share information in the event of a child death. For more information please see the Berkshire Child Death Overview Panel (CDOP) website: http://www.bhps.org.uk/cdop/home.html

Sharing data and information to support organisations in their duty to safeguard

This list is not exhaustive.

- Flagging on IT systems – children with Child Protection plans and Looked After Children
- Provision of appropriate care services
- Monitoring and protecting public health, improving the health of the population
- Managing and planning services (where data has been suitably anonymised)
- Commissioning and contracting services (where data has been suitably anonymised)
- Developing inter-agency strategies
- Performance management, audit and quality assurance
- Research (subject to the Research Governance Framework)
- Investigating complaints or serious incidents
- Reducing risk to individuals, service providers and the public as a whole e.g. Domestic Abuse data with Community Safety Officers
- Staff management and protection e.g. Local Authority Designated Officer (LADO)
- Statutory inspections

2. LEGAL CONTEXT OF INFORMATION SHARING

There is no general statutory power to share information, just as there is no general power to obtain, hold or process data.

The Data Protection Act 1998 governs the obtaining, holding and processing of personal information while some Acts of Parliament give public bodies 'express statutory powers' to share information. These are often referred to as 'statutory gateways' and are enacted to provide for the sharing of information for particular purposes.

The Human Rights Act 1998 and the European Convention of Human Rights

The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable action within their powers (which would include information sharing) to safeguard the Convention rights of children. These rights include Article 8, and recognise a right to respect for private and family life:

Common law duty of confidentiality

The common law duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to.

Data Protection Act 1998

This Act deals with the processing of personal (i.e. sensitive and non-sensitive) data.

Personal data is data which relates to a living person, including the expression of any opinion or any indication about the intentions in respect of the child or young person is considered personal data. Sensitive personal data is personal data relating to racial or ethnic origin, religious or other similar beliefs, physical or mental health or condition, sexual life, political opinions, membership of a trade union, the commission or alleged

commission of any offence, any proceedings for any offence committed or alleged to have been committed, the disposal of proceedings or the sentence of any court in proceedings.

Organisations which process personal data must comply with the data protection principles set out in schedule 1 of the Act.

Specific legislation containing express powers or which imply powers to share Information

The Children Act 1989

Sections 17 and 47 of the Children Act 1989 place a duty on local authorities to provide services for children in need and make enquiries about any child in their area who they have reason to believe may be at risk of significant harm.

Sections 17 and 47 also enable the local authority to request help from other local authorities, education and housing authorities and NHS bodies and places an obligation on these authorities to co-operate.

The Act does not require information to be shared in breach of confidence, but an authority should not refuse a request without considering the relative risks of sharing information, if necessary without consent, against the potential risk to a child if information is not shared.

The Children Act 2004

Section 10 of the Act places a duty on each Children's services Authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children and young people from pre-birth to 19 years (25 in case of those with disabilities) in their area.

Relevant partners must cooperate with the local authority to make arrangements to improve children's wellbeing.

This statutory guidance for section 10 states that good information sharing is key to successful collaborative working and that arrangements under section 10 of the Act should ensure that information is shared for strategic planning purposes and to support effective service delivery.

It also states that these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations.

Section 11 of the Act places a duty on key people and bodies to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children.

The section 11 duty does not give agencies any new functions, nor does it override their existing functions, it simply requires them to:

- Carry out their existing functions in a way that takes into account the need to safeguard and promote the welfare of children;
- Ensure that the services they contract out to others are provided having regard to that need.

In order to safeguard and promote the welfare of children, arrangements should ensure that:

- All staff in contact with children understand what to do and the most effective ways of sharing information if they believe a child and family may require targeted or specialist services in order to achieve their optimal outcomes;

- All staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including those children suffering or at risk of significant harm.

Education Act 2002

The section 11 duty of the Children Act 2004 mirrors the duty placed by section 175 of the

Education Act 2002 on LAs and the governing bodies of both maintained schools and further education institutions to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children and follow the guidance in Safeguarding Children in Education (DfES 2004).

The guidance applies to proprietors of independent schools by virtue of section 157 of the Education Act 2002 and the Education (Independent Schools Standards) Regulations 2003.

Education Act 1996

Section 13 of the Education Act 1996 provides that an LA shall (so far as their powers enable them to do so) contribute towards the spiritual, moral, mental and physical development of the community, by securing that efficient primary and secondary education is available to meet the needs of the population of the area. Details of the number of children in the local authority's area and an analysis of their needs is required in order to fulfil this duty so there may be an implied power to collect and use information for this purpose.

Section 434 (4) of the Act requires LAs to request schools to provide details of children registered at a school.

Learning and Skills Act 2000

Section 117 provides for help to a young person to enable them to take part in further education and training. Section 119 enables Connexions services to share information with the Benefits Agency and Jobcentre Plus to support young people to obtain appropriate benefits under the Social Security Contributions and Benefits Act 1992 and Social Security Administration Act 1992.

Education (SEN) Regulations 2001

Regulation 6 provides that when the LEA are considering making an assessment of a child's special educational needs, they are obliged to send copies of the notice to social services, health authorities and the head teacher of the school (if any) asking for relevant information.

Regulation 18 provides that all schools must provide Connexions Services with information regarding all Year 10 children who have a statement of special educational needs.

Children (Leaving Care) Act 2000

The main purpose of the Act is to help young people who have been looked after by a local authority move from care into living independently in as stable a fashion as possible. To do this it amends the Children Act 1989 (c.41) to place a duty on local authorities to assess and meet need. The responsible local authority is to be under a duty to assess and meet the care and support needs of eligible and relevant children and young people and to assist former relevant children, in particular in respect of their employment, education and training. Sharing information with other agencies will enable the local authority to fulfil the statutory duty to provide after care services to young people leaving public care.

Protection of Children Act 1999

The Act creates a system for identifying persons considered to be unsuitable to work with

children. It introduces a 'one stop shop' to compel employers designated under the Act (and allows other employers) to access a single point for checking people they propose to employ in a child care position. This will be achieved by checks being made of criminal records with the National Criminal Records Bureau and two lists maintained by the Department for Children, Schools and Families.

Immigration and Asylum Act 1999

Section 20 provides for a range of information sharing for the purposes of the Secretary of State:

- To undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act;
- To undertake the provision of support for asylum seekers and their dependents.

Local Government Act 2000

Part 1 of the Local Government Act 2000 gives local authorities powers to take any steps which they consider are likely to promote the wellbeing of their area or the inhabitants of it. Section 2 gives local authorities 'a power to do anything which they consider is likely to achieve any one or more of the following objectives:

- The promotion or improvement of the economic wellbeing of their area;
- The promotion or improvement of the social wellbeing of their area;
- The promotion or improvement of the environmental wellbeing of their area.

Section 2 (5) makes it clear that a local authority may do anything for the benefit of a person or an area outside their area, if the local authority considers that it is likely to achieve one of the objectives of Section 2(1).

Section 3 is clear that local authorities are unable to do anything (including sharing information) for the purposes of the wellbeing of people - including children and young people - where they are restricted or prevented from doing so in the face of any relevant legislation, for example, the Human Rights Act and the Data Protection Act or by the common law duty of confidentiality.

Criminal Justice Act 2003

Section 325 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.
- 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
    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).
- In establishing those arrangements, the responsible authority must act in co-operation with the persons identified below. Co-operation may include the exchange of information.

Crime and Disorder Act 1998

Section 17 applies to a local authority (as defined by the Local Government Act 1972); a joint authority; a police authority; a national park authority; and the Broads Authority. As amended by the Greater London Authority Act 1999 it applies to the London Fire and

Emergency Planning Authority from July 2000 and to all fire and rescue authorities with effect from April 2003, by virtue of an amendment in the Police Reform Act 2002.

It recognises that these key authorities have responsibility for the provision of a wide and varied range of services to and within the community. In carrying out these functions, section 17 places a duty on them to do all they can to reasonably prevent crime and disorder in their area.

National Health Service Act 1977

The Act provides for a comprehensive health service to England and Wales to improve the physical and mental health of the population and to prevent, diagnose and treat illness.

Section 2 provides for sharing information with other NHS professionals and practitioners from other agencies carrying out health service functions that would otherwise be carried out by the NHS.

Health Act 1999

Section 27 of the Health Act replaces section 22 of the NHS Act 1977. Section 27 states that

NHS bodies and local authorities shall cooperate with one another (this allows for practitioners to share information) in order to secure the health and welfare of people.

Health and Social care Act 2012

The Health and Social Care Act 2012 underpins wide ranging reforms of the NHS since it was founded in 1948. Changes include the establishment of a National Health Service Commissioning Board and Clinical Commissioning Groups, as well as Health and Wellbeing Boards. The changes became operational on 1st April 2013. The Act sets out provision relating to public health in the United Kingdom; public involvement in health and social care matters; scrutiny of health matters by local authorities and co-operation between local authorities and commissioners of health care services. The Act establishes a National Institute for Health and Care Excellence, and establishes the provision for health and social care.

The clinical commissioning organisations established by the Act must have a secure legal basis for every specific purpose for which they wish to use identifiable patient data. Where there is no such statutory legal basis either the consent of the patient is required to process personal confidential data or the data must be fully pseudonymised.

The Adoption and Children Act 2002

For further information about the Adoption and Children Act 2002 and Regulations see

www.education.gov.uk/childrenandyoungpeople/families/adoption

3. BERKSHIRE DATA AND INFORMATION SHARING AGREEMENT

Partners to this Agreement

This Information Sharing Agreement has been approved by all partner members of the six Berkshire Local Safeguarding Children Boards.

Purpose

The aim of this agreement is to facilitate the lawful exchange of personal and sensitive data in any form, within and between organisations for notified and defined purposes, respecting the rights of individuals set out in legal acts and common law. When the records of deceased people are required by their relatives or other parties, ethical and confidentiality issues will be safeguarded in the same way as if the person was living.

The public expects and the Data Protection Act 1998 requires that personal information held by statutory agencies will be properly protected. However, there is also a public expectation that there will be an appropriate sharing of information in working in partnerships for specific pieces of work with statutory obligations.

The purpose of sharing information between partner organisations is to:

- Ensure the provision of appropriate services for children and young people in need or at risk or likely to be at risk of suffering significant harm: sections 17 (10) and 47 (1) of the Children Act 1989 - or who otherwise are considered to be at risk of social or educational
  exclusion.
- Obtain the assistance for the local authority from other local authorities, in order for the local authority to perform its functions of providing services to children, young people and families under Part 111, Section 27, Children's Act 1989.Promote or improve the economic, social or environmental well being of children, young
  people and families in need in Bracknell Forest. This will include the provision of improvements to health and/or educational opportunity as well as the reduction or elimination of risk factors for children and young people within the city.
- Prevent or reduce crime and identify and apprehend offenders or suspected offenders Section 115, Crime and Disorder Act 1998.
- Ensure that children and young people who are missing education or at risk of going missing from education, are identified and supported.
- Provide information to assist in the planning and development of services for children and young people.
- Provide information for statistical analysis.

By sharing information, partner organisations will be able to identify children and young people considered to be in need or at risk of social or educational exclusion at an early stage of concern and provide effective multi-agency intervention in order to promote their health and well-being. Nominated representatives from organisations which are signatories to this agreement will be engaging in regular, multi-agency discussions in order to secure services for identified children, young people and their families.

The type and extent of information to be shared

Routine information sharing

The information shared will be the minimum amount necessary; it will be relevant and only used for the purposes of this agreement.

This is necessary to ensure compliance with the second and third principles of the Data Protection Act 1998:

Principle 2: "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

Principle 3:" Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

Anonymised information

Whenever possible data should be anonymised, if large volumes of data is provided for Management Information (MI), research and/or planning by partner organisations, as a matter of courtesy the outcome of that research/planning should be provided to the organisation(s) supplying the data.

Data Sharing Categories

Aggregated/Statistical Information - aggregate and management information to plan and monitor progress of the service. This information can be shared without client consent.

De-Personalised/Anonymous Information - Individual level information may be depersonalised/ anonymised by the removal of any client identifiable information (such as name, address, unique identifiers, etc) and therefore outside the ambit of the Data Protection Act 1998, then shared by organisations within the context of this protocol. This information can be shared without client consent.

Personal Non Confidential/Non Sensitive Information - Information needed to identify and maintain contact with all clients in order to provide an effective service, such as Name, Address and Date of Birth. This information may be shared with the Informed Consent of the client.

Personal Confidential/Sensitive Information - Information needed to provide comprehensive support to clients and can be subdivided into broad categories:

Confidential - This information deemed to be 'professionally' sensitive, such as client characteristics (e.g. homeless, substance misuse, etc), assessment data or opinions.

Sensitive - This is information defined within the Data Protection Act 1998 as sensitive such as ethnicity, religious beliefs, criminal procedures or health related issues.

Confidential and/or sensitive information cannot be shared unless the client has given their Explicit Consent. There is other overriding legislation and exceptional circumstances.

Data Quality

Information held must be accurate and kept up to date. Steps must be taken to validate information, such as checking with the person who originally provided the information, if there
is any doubt as to its accuracy. Sharing inaccurate information can lead to decisions being made on false information. Data owners will ensure they amend any incorrect details and inform partners of the correct information.

Information discovered to be inaccurate, out-of-date or inadequate for the purpose should be notified to the Data Controller who will be responsible for correcting the data and notifying all other recipients of the information who must ensure the correction is made.

Designated Officer

In order to ensure compliance with the Data Protection Act, participants to this Agreement shall nominate a Designated Officer to whom all requests and from whom all disclosures of personal information will be made.

Disclosure requests, disclosure decisions and the details of personal information that has been disclosed will be in writing and the designated officer will maintain a record. The identity of the data owner must also be recorded against the relevant data. No secondary use or other use may be made unless the consent of the disclosing party to that secondary use is sought and obtained.

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data. The data owner will then notify all other recipients of that data, who must ensure that the correction is applied. Decisions on disclosures reached at meetings must be minuted.

The designated officer will ensure that appropriate security arrangements are in place within their respective organisations to prevent unauthorised access to and disclosure of personal data.

A list of designated officers will assume responsibility for data protection, security and confidentiality issues and compliance with legislation within their respective organisations will be made available to partner organisations as a matter of routine.

Disclosures and Transfer of Information

Where information is shared, disclosed or exchanged requests for information will be specific to the purpose, recorded and made on a need to know basis.

When disclosing personal information, many of the data protection issues surrounding disclosure can be avoided if the consent of the individual concerned has been sought and obtained.
The organisation that originally discloses personal information to another party to this Agreement always retains ownership of the data (the data owner), each organisation must therefore decide the propriety of any particular disclosure. The identity of the data owner must always be recorded against that data.

A recipient of personal information must obtain the consent of the data owner before making a secondary disclosure to another party to this Agreement. For the purpose of this requirement, each council department will be treated as a separate organisation.

Partner organisations will have appropriate information systems and records about information transfers. These records should cover when information has been given, when it has been refused and what medium has been used, including paper, electronic and conversational. The records should also cover the disposal and amendment of information. Where information is exchanged on a case by case basis, it should be ensured that requests are specific and recorded. Disclosure of information should be authorised by the appropriate personnel and should be provided on a need to know basis only. This "need to know" principle is a fundamental part of ensuring information is shared appropriately and is in compliance with the Data Protection Act 1998.

Data retention, review and disposal

Partner organisations will apply relevant regulations and timescales to the retention, review and disposal of information, (electronic and paper based), only keeping information for as long as is necessary in relation to the original purpose

Appropriate Security

General

The partners to this agreement acknowledge the security requirements of the Data Protection Act 1998 applicable to the processing of the information subject to this agreement.

Each partner will make sure they take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In particular, each partner must make sure they have procedures 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 way that makes reconstruction unlikely.
- Promote discretion to avoid unauthorised access.

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

Additional arrangements

To determine what security measures are appropriate in any given case, partners must consider the type of data and the harm that would arise from a breach of security.

Information obtained in confidence may be regarded as requiring a higher level of security. In particular, they must consider:

- Where the information is stored.
- The security measures programmed into the relevant equipment.
- The reliability of employees having access to the information.

Complaints and breaches

All complaints or breaches relative to this agreement will be notified to the designated Data Protection Manager of the relevant organisation in accordance with their respective policy and procedures. Partner organisations will need to have appropriate arrangements to:

- Tackle any breach of agreement.
- Handle internal discipline.
- Monitor security incidents.
- Deal with malfunctions.

Indemnity

In return for the provision of any information by a partner organisation to another (the Receiving Partner) under the terms of this Agreement, the Receiving Partner undertakes to indemnify the Partner that provided the information in respect of all claims and liabilities arising from the use of the information by the Receiving Partner or it's failure to comply with its obligations under the Agreement.

Subject Access Requests

All Subject Access Requests must be made in writing to the relevant data controller and the subsequent actions taken must be fully recorded within the organisation's system.

Information obtained from a partner organisation without the prior consent of the data subject cannot be disclosed to that individual without the agreement of the originating organisation. This does not prevent the individual making a separate Subject Access Request to the originating partner organisation. Agencies must make sure that data will be received by the requester no later than 40 days from receipt of request.

Children under 12 years of age

When a child does not have the capacity to understand the request, a parent/ guardian/carer can make a Subject Access Request in respect of their child.

Information on consent and Fraser competence guidelines are attached as annex 1 of this document.

Parent/guardian/carer

Parents/guardians/carers of individuals with sufficient understanding of their rights have no automatic rights of access to the subject's data (in accordance with Data Protection Act 1998) It is considered good practice to ensure that the parent/guardian/carer of those under 16 years old is informed that the gathering, recording and possible sharing of information is taking place.

Parents/guardians/carers will normally only be able to access an individual's data (if they are deemed competent) with the signed consent of the subject.

All parent/guardian/carer requests to access data must be referred to the designated manager within the relevant organisation.

Access may be granted in cases where the designated manager is satisfied that an individual is not capable of representing themselves and that the parent/guardian/carer constitutes the client's legitimate representative.

Where a Subject Access Request has been granted to the parent/guardian/ carer the reasons for doing so must be fully recorded and clearly referenced to the evidence and information on which the decision is made

Freedom of Information Act considerations

If a party receives a request for information under the Freedom of Information Act 2000 and the information requested is identified as belonging to another signatory party, it will be the responsibility of the receiving agency to contact that party to determine whether the latter wishes to rely on any statutory exemption under the provisions of the Freedom of Information Act 2000 and to identify any perceived harm.

General operational guidance

Partner organisations must consider the staff time and resource implications that are involved for the Data Controller extracting the data. If a request is made and then the data is no longer required there should be a process for withdrawing the request.

Partner organisations to this agreement will need to identify:

- A named individual to lead on the Agreement
- How they will champion training on the Agreement.

Partners will work within the accompanying Operational Agreement and Arrangements governing the collection, transfer, storage and disposal of information.

Review Arrangements

This Information Sharing Agreement will be formally reviewed annually unless legislation or

government guidance necessitates an earlier review. Any of the signatories to the Agreement can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

Closure/termination of agreement

Any partner organisation can suspend the Information Sharing Agreement for 30 days, if they feel that security has been seriously breached. This should be done in writing and evidence provided.

Any suspension will be subject to a risk assessment and resolution meeting, comprising of the signatories of this agreement or their nominated representative. This meeting will take place within 14 days of any suspension.

Signatories to this Agreement:

Agency / Organisation
Bracknell Forest Council
Youth Offending Service
Thames Valley Police
NHS Berkshire East Clinical Commissioning Group
Berkshire HealthCare NHS Foundation Trust
NHS Central Southern Commissioning support Unit
National Probation Service
Probation(Thames Valley Community Rehabilitation Company)
Bracknell and Ascot Clinical Commissioning Group
Involve – Bracknell Forest
CAFCASS confirmed

PART 2 – Template for developing an Information Sharing Agreement on specific areas of work

SERVICE / PROJECT SPECIFIC INFORMATION SHARING AGREEMENT

(Put in here description of service of subject of agreement :)

PURPOSE OF THE AGREEMENT

The purpose of this agreement is to provide the framework to enable lawful exchange of personal and sensitive data in any form, within and between the specified organisations. This is an agreement between XXX and XXX_.

It is made under the auspices of the Bracknell Forest Data and Information Sharing Protocol for Agencies Working with children and Young People.

The Data Protection Act 1998 requires that personal information held by statutory agencies will be properly protected.

PARTIES TO THE AGREEMENT

The parties to this agreement are:

INFORMATION ABOUT THE SERVICE

(In this section the lead manager should provide details about the project / service and include: A clear statement of why there is a need to share information between the organisations party to this Information Sharing Agreement.)

DATA ITEMS TO BE SHARED

In this section specify:

- What data / information will be shared?
- How will the data / information be shared?
- How will the information be stored / secured?
- How will consent be gained (if appropriate) and how will this be recorded?
- If consent is not gained need to say why and record clearly.

Data Sharing Requests

(The service will have an agreed set of data that it will routinely share with the parties to this agreement in order to provide evidence of performance management linked to the service objectives / targets.)

(Where data is being requested of the service which is in addition to the data agreed by all parties a data request form will be completed and returned to xxxxxxxxxxxx.)

A data request form is attached as annex 3

A decision will be made about the data request by the lead manager and will then be processed accordingly.

BASIS FOR SHARING INFORMATION

The Data Protection Act 1998 governs the obtaining, holding and processing of personal information while some Acts of Parliament give public bodies express statutory powers to share information.

For the purpose of this framework the key legislation informing the work of the XXX includes:

- Insert here the key legislation that underpins the service being provided.

ACCESS AND INDIVIDUALS RIGHTS

(Lead manager to determine who will have access to the information within the parties signed up to the agreement.)

(Where a project is hosted by one agency / authority the service will operate under the policies and procedures of the host agency / authority.)

Freedom of Information Requests

The parties in this agreement are subject to legal duties under the Freedom of Information Act and any other applicable legislation governing access to information.

Each party in the agreement will assist the others to enable compliance with the obligations. All parties in the agreement are entitled to any and all information relating to the performance of the agreement.

INFORMATION GOVERNANCE

Governance of the service will be the responsibility of the Lead Manager / Management Board who will be responsible for the agreement of service delivery outputs and outcomes and for monitoring all aspects of the service.

The following areas will need to be considered for this section:

Agreement about what datasets will be shared to ensure it is reasonable / and not too excessive.

- Looking at ways to ensure the quality of the data, and the accuracy of the data.
- Ensuring consistency of data recording and ensuring compliance with the data sharing agreement and policies and procedures.
- Agree the retention and destruction processes of shared items and a process for dealing with potential challenges if there is disagreement.
- Agree the security and storage arrangements and a process for dealing with any breaches.
- Agree a process for dealing with FOI and data requests.
- Agree a process for keeping data and information sharing under review.
- Agree timescales for review of agreement

INFORMATION SECURITY

The parties to this agreement acknowledge the security requirements of the Data Protection Act 1998 applicable to the processing of the information subject to this agreement.

Each partner will make sure that they take appropriate technical and organisational measures against unauthorised or unlawful processing around personal data and against accidental loss or destruction of, or damage to, personal data.

In particular each partner must ensure they have procedures in place to ensure that all reasonable steps are taken to:

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

Access to information subject to this agreement will only be granted to those professionals who "need to know" to effectively discharge their duties.

To determine what security measures are appropriate in any given case, the parties to this agreement must consider the type of data and what risk /harm there would be in the event of a security breach.

Key to the process is considering:

- Where the information will be stored
- The appropriate level of security measures within the ICT equipment
- The training of all staff in information security and data protection.

REVIEW ARRANGEMENTS

This Information Sharing Agreement will be reviewed by xxx at least annually and more frequently where there are significant changes to the service.

Information Sharing Agreement Signed

Name	Role	Organisation

Date Signed:	
First Review Date:	
Second Review Date:	

Part 3: Annex Information

Annex 1: Consent and Fraser Competence Guidelines

In many instances, you will seek consent to share information from the parent/ carer. This is particularly the case in work with younger children and in any interventions which include support work with the family. However in some cases the child/young person will be able to give consent without referral to their parent/carer. This is possible if they are judged to be Fraser Competent.

Children under 16 should always be encouraged to involve their parent/carer unless to do so could put them at risk of harm. Particular care should be taken with children with a disability, who are sometimes wrongly assumed not to be able to give consent.

The term, 'Fraser competent', arises from the case in the 1980s when Victoria Gillick attempted to set a legal precedent which would have meant that medical practitioners could
not give young people under the age of 16 treatment or contraceptive services without parental permission. (Gillick vv West Norfolk and Wisbech Area Health Authority, 1985)

The ruling was initially successful but then the House of Lords ruled that young people who are under 16 are competent to give valid consent to a particular intervention if they have sufficient understanding and intelligence to enable them to understand fully what is proposed
and are capable of expressing their own wishes. Lord Fraser was the leading Law Lord for the review.

Although the ruling was initially in regard to medical consent, it is now generally felt that the ruling applies to consent for other services.

Annex 2: Caldicott Principles

Caldicott Report 1997 – And the Caldicott 2 Review 2013

In December 2011 the Government announced that it wanted to allow patients' records and other NHS data to be shared with private life science companies, to make it easier for them to develop and test new drugs and treatments. Concerns were raised about what that might mean for patient confidentiality. This and other issues prompted the instigation of Caldicott 2, in which Dame Fiona was asked to review information issues across the health and social care system.

Dame Fiona first investigated issues surrounding confidentiality when she chaired a similar review in 1996-7 on the use of patient data in the NHS. That review recommended that the NHS adopt six principles (see below) for the protection of confidentiality, which became known as the "Caldicott principles". The review also recommended that NHS organisations appoint someone to take responsibility for ensuring the security of confidential information. These people became known as "Caldicott Guardians".

The reach of Caldicott 2 is far wider than the 1997 report. Its recommendations affect all organisations working in the health and social care sector – including local authorities. Its recommendations, if adopted, will have a significant impact on the way that local authorities operate.

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

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

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

4. Access should be on a strict need to know basis - Only those individuals who need access to patient-identifiable information should have access to it. They should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

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

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

The new Caldicott principle,

The duty to share personal confidential data can be as important as the duty to respect service user confidentiality. Registered social workers working with a patient should be considered to be part of the patient's care team. This means that the patient is taken as having given their implied consent to relevant information being shared with the social worker for the purpose of their care.

Only the NHS and Social Care are required to apply these principles and to nominate a senior person to act as a Caldicott Guardian responsible for safeguarding the confidentiality of patient information.

Annex 3: Data Request Form in relation to xxx service / project

In requesting information and signing this request you are agreeing to comply with the principles of the Data Protection Act 1998.

The Data Protection Act is not a barrier to sharing information, but provides a framework to ensure that personal information is shared appropriately and securely.

All requests for information / data will be assessed against the rules for information sharing, and against relevant legislation and guidance, and where relevant legal advice will be sought before a decision is made to share.

Name of requester: *(NB this is the person to whom the data/information will actually be sent)*	
Job Title:	
Organisation:	
Date request submitted:	
Deadline/date required: *(NB Please be as realistic as possible or put 'to be discussed'. If you write 'asap' we will contact you anyway to discuss)*	

Tel:	
e-mail (if external): ***(***please note all information will be sent via electronic means through either GCSX or through an encrypted email, information will not be sent if it is considered insecure to do so)	
Details of data/information required: *(please be as specific as possible about breakdown (eg child/school/Borough level) and format (eg spreadsheet map/chart etc)If spreadsheet ideally please supply a list of the headings you need or a template in Excel)*	
Frequency that data is required ***(***please specify if this is a one off request or if this is a regular requirement, and note that this will be kept under review to ensure ongoing data protection compliance)	
Purpose data will be used for: *(this will not only enable us to prioritise requests but also help us understand and anticipate future requirements)*	
Confidentiality /Data Protection? *(is the information likely to lead to anyone being identifiable? Where will it be stored once it is sent to you?)*	
Any additional information? *(eg is this for an FOI request? Is it a statutory requirement? Is the request a one-off or a regular requirement?)*	

Please submit your data request to:

Xxxxxxxx

Email address

Annex 4: Useful Information Links

HM Government: Information Sharing: Advice for Practitioners providing safeguarding services to children, young people, parents and carers.	https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice
Information Commissioners Office (ICO)	https://ico.org.uk/
NHS: Inter-agency information sharing protocol	http://www.this.nhs.uk/fileadmin/IG/interagency-information-sharing-protocol.pdf