***Medway is Promoting Practice***

***It’s our practice that will make the difference***



**MEDWAY**

**MULTI-AGENCY**

**SAFEGUARDING HUB**

**STANDARD OPERATING PROCEDURES**

**January 2019**

|  |  |
| --- | --- |
| **Document Author** |  Louise Drury |
| **Document Owner** | Director Children and Adult Services |
| **Summary of Purpose** | This MASH Operational Protocol is aimed at all participating staff and agencies. It maps out the child’s journey through the MASH. The protocol will be included in the induction of any new MASH members. |
| **Review date** | April 2019 |
| **Accessibility** | This document can be made available in large print, or in electronic format. There are no copies currently available in other languages |
| **Equalities Impact Assessment** | During the preparation of this policy and when considering the roles and responsibilities of all agencies, organisations and staff involved, care has been taken to promote fairness, equality and diversity in the services delivered, regardless of disability, ethnic origin, race, gender, age, religious belief or sexual orientation. These issues have been addressed in the policy by the application of an impact assessment checklist. |
| **Circulation Restrictions** | None |
| **Version** | **Detail of change** | **Date** |
| **1.0** | Document Created | March 2018 |
| **2.0** | Document reviewed by the MASH Strategic Board and amended. | April / June 2018 |
| **3.0** | Document reviewed by the MASH Strategic Board and amended. | January 2019 |

**Contents Page**

**1** [**Introduction**](#_Introduction) **4**

**2 Governance 5**

**3 Consent 5**

**4 Definition of MASH 6**

**5 Functions and Outcomes of MASH 7**

**6 MASH Information Gathering and Analysis Process 7**

**7 SPA and MASH Meetings 9**

**8 MASH Location and Partner Agencies 9**

**9 Dispute Resolution and Escalation 11**

**10 Evaluation and Quality Assurance of MASH 12**

**11 Management of Specific Issues in MASH 12**

**Appendices**

**Appendix 1 Referral and Contact Pathway 17**

**Appendix 2 MASH Roles and Responsibilities 18**

**Appendix 3 MASH Partner Agency Profiles 20**

**Appendix 4 Information Sharing Agreement 26**

**Appendix 5 List of MASH Professional Lead Contacts 55**

**INTRODUCTION**

Safeguarding children requires a high level of interagency co-operation and information sharing in order to build an accurate picture of the child’s circumstances, need for additional support and to identify risks of harm. Medway safeguarding partners have developed the Multi-Agency Safeguarding Hub (MASH) as an arrangement that will fulfil the statutory requirement for co-operation to ensure that the Local Authority is able to meet and deliver safeguarding outcomes. Medway MASH went live on 9th April 2018.

This MASH Operational Protocol is aimed at all participating staff and agencies. It maps out the child’s journey through the MASH. The protocol will be included in the induction of any new MASH members.

The Medway approach to safeguarding is to **ensure access to the right support at the right time.** This approach is underpinned by the following key principles:

* **Access**: services to be focused around the needs of children, young people and families, rather than institutional/agency boundaries.
* **Early intervention**: effective early identification and assessment with appropriate intervention will reduce the need for more costly, and possibly less successful, provision later.
* **Reducing dependency**: working with families at all levels of need to reduce dependency and promote self-reliance and resilience, therefore enabling problem solving within the family.
* **Shared responsibility and response:** getting the best for children is everyone’s business and services need to develop a shared responsibility and response to children, young people and their families.
* **Participation and involvement**: children, young people and families should be active participants in designing, planning and reviewing the services they receive.
* **Equality of opportunity:** services should continue to work together to remove the cultural, geographical and economic barriers to opportunity, which some children and young people face.
* **Services based on clear evidence:** planning and delivery of services should be informed by robust data that evaluates what works and achieves the best outcomes for children and families.

**GOVERNANCE**

The MASH is governed under the Children’s Safeguarding Service Structure and aligned to the Medway Safeguarding Children’s Board (MSCB).

The governing forum that oversees the MASH and associated activities, amendments to processes and protocols, quality assurance etc. is the MASH Strategic Group – chaired by Deputy Director. The MASH Operational Group – chaired by Head of Service Safeguarding, is responsible for evaluating and troubleshooting any matters compromising the MASH operational functioning.

The document should be read in conjunction with the following related documents:

* **MASH Information Sharing Agreement** and
* **Medway Inter-Agency Threshold Criteria for Children in Need.**

**CONSENT**

Consent is the key to successful information sharing. For all assessment, it is important that consent is obtained where it is sensible, in the child's best interest, and practical. Even where the Data Protection Act does not demand it, operating with consent is good practice.

To give informed consent, a child/young person and/or their parent/carer must be entirely clear about the purpose of the information; how it will be used; who it may be shared with and how it will be shared; how long it will be held and in what form. *This must include making them aware of circumstances where information may be shared without consent and where confidentiality cannot be maintained.*

Consent can be withdrawn at any time: giving of consent is not a one-off event. It is a continuous and ongoing issue that needs to be revisited at regular and reasonable intervals. The child/young person and/or their parent/carer should be informed that they can withdraw consent at any time.

There may be circumstances when consent can be overridden to share information.

“The key factors in deciding whether or not to share confidential information are necessity and proportionality, i.e. whether the proposed sharing is likely to make an effective contribution to preventing the risk and whether the public interest in sharing information overrides the interest in maintaining confidentiality”

*Information Sharing: Guidance for practitioners and managers. DCSF p21.*

There are some circumstances where sharing information without consent will be justified in the public interest. These are:

1. when there is evidence or reasonable cause to believe that a child is suffering, or is at risk of suffering, significant harm; or
2. to prevent significant harm to a child, including through the prevention, detection and prosecution of serious crime.[[1]](#footnote-1)

When there is justifiable public interest, there are some circumstances where consent can be overridden, furthermore there may also be times when it is also NOT appropriate to inform the child/parent or person with parental responsibility that the information will be shared. If doing so would:

1. place a person at increased risk of significant harm; or
2. prejudice the prevention, detection or prosecution of a serious crime; or
3. lead to an unjustified delay in making enquiries about allegations of significant harm to a child.[[2]](#footnote-2)

A decision to override consent in these circumstances will be need to be agreed between the SPA and MASH Practice Manager and the agency who owns the information. The rationale and decision must be clearly recorded on the contact record.

**DEFINITION OF MASH**

The Multi-Agency Safeguarding Hub is an environment where partnership agencies with the duty to safeguard children are co-located. Co-location enables safe, speedy and efficient information sharing and professional discussions to assist children services to make a quick and evidence based decision on the level of risk and need involved and on how to best safeguard/support children and their families – that being universal services, single agency support, co-ordinated support via the common assessment framework process, early intervention and prevention, child in need support or initiating child protection procedures.

The Multi-Agency Safeguarding Hub members co-operate on a day-to-day basis by sharing information in a fire walled facility. On specific cases – identified by the MASH decision maker using the agreed RAG rating risk assessment tool – each partner agency will research their own database and data and provide the research in written format to the MASH decision maker. All information that is shared by agencies as a part of the MASH confidential screening is stored on a secure database and accessible by the delegated MASH children social care staff only.

**FUNCTIONS OF THE MASH**

The MASH helps deliver three key functions:

Information based risk assessment and decision-making

Identify through the best information available to the safeguarding partnership those children and young people who require support or a necessary and proportionate intervention.

Victim identification and harm reduction

Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions.

Co-ordination of all safeguarding partners

Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and co-ordination of harm reduction strategies and interventions.

**MASH INFORMATION GATHERING AND ANALYSIS PROCESS**

The Single Point of Access receives all safeguarding contacts and referrals. Not all cases referred to the Single Point of Access will go through the MASH process. The SPA threshold screening will be applied to determine which cases require additional information to make threshold decision and ensure that a child is safe.

* The SPA and MASH Practice Manager will screen and prioritise those contacts for MASH information sharing using a RAG rating (Red/Amber/Green) (not all referrals will go through the MASH process).
* Staff from every agency in MASH will gather and share securely information (through completing the Framework i information request form) to enable an informed decision to be made.
* The SPA and MASH Practice Manager will use the collected information to make a decision about the most appropriate intervention(s) for the child’s identified needs.
* The team receiving the case will receive a summary of the relevant information and feedback will be provided on outcome of MASH process to the referrer.

Timescales

* Red: will be prioritised with information from MASH partners expected to be available within 4 hours.
* Amber: Decision made within 1 working day include information sharing by MASH.
* Green: Decision made within 1 working day.

***Please see Appendix 1 – Contact and Referral Pathway***

**SPA AND MASH MEETINGS**

**SPA Huddle**

Every morning at 9.15am there is a meeting led by the SPA and MASH Practice Manager and attended by Referral and Information Officers, SPA Social Worker, Early Help Social Worker and MASH DS to review any work from the previous day and work that may have been received on the Portal, from Police and Out of Hours Service overnight. The team also update on staffing to ensure sufficient capacity to manage the daily tasks and incoming contacts.

**MASH Huddle**

Every morning at 9.30am there is a meeting led by the SPA and MASH Practice Manager, attended by MASH Social Workers and partners to review any work from the previous day and work that has been received on the Portal, from Police and Out of Hours Service overnight. The team update on staffing to ensure sufficient capacity to manage the daily tasks and incoming work.

**MASH Meetings**

MASH meetings take place twice a day at 11.30am and 3.00pm led by the SPA and MASH Practice Manager and attended by the allocated MASH social Work and MASH partners who have provided information in response to the MASH Enquiry. The Early Help co-ordinator attends all MASH meetings to ensure that every contact and referral is considered for Early Help Services .The outcome of the discussion is recorded on the child’s contact and referral episode and Partners are responsible for updating their own records regarding the outcome.

**MASH LOCATION AND PARTNER AGENCIES**

Medway MASH is located on the 1st floor Broadside, Leviathan Way, Chatham, ME4 4LL.

Contact details:

Customer First - 01634 **334466**

The Portal for the Single Point of Access can be found [Here](https://www.medway.gov.uk/info/200170/children_and_families/600/worried_about_a_child/1) or at the following address:

<https://www.medway.gov.uk/info/200170/children_and_families/600/worried_about_a_child/1>

For concerns out of hours the contact number is **03000419191**

In the case of emergencies, call the Police: 999

The following agencies Medway MASH partners. The dedicated MASH professional from each agency work as part of the MASH team and provide information from their agency database. Some agencies are co-located core members of the MASH team, while others are satellite members who are not co-located but provide information from agency databases at the request of the MASH. All core partners share information electronically via Framework i (apart from health, police).

Core partners

Children Social Care

Police

Health

Education

Early Help

Virtual Partners

Housing

Youth Offending Service

Turning Point (Drug and Alcohol services)

Adult Social Care

Probation NPS

Probation CRC

***See Appendix 2 for MASH Roles and Responsibilities***

***See Appendix 3 for the details of the individual MASH Partner Agency Profiles.***

***See Appendix 4 Information Sharing Protocol.***

***See Appendix 5 for the list of MASH Professional Lead contacts.***

Availability and Cover Arrangements

* Full-time MASH team members are expected to be available between 9am and 5.15pm Monday to Thursday and 9am and 4.45pm on Friday.
* In the event of any MASH agency member being unavailable on any day, their originating agency will be responsible for ensuring suitable cover is available and will ensure that the SPA and MASH Team Manager is advised at the earliest opportunity.

Management, supervision and training of MASH team members

Originating agencies remain responsible for the line management and supervision of individual MASH team members in line with the originating agency’s own policies and as set out in the MASH Governance Arrangements. This includes identifying and meeting the worker’s needs.

Agencies are responsible for ensuring staff has received suitable training to enable them to carry out their MASH role. Core training should include:

* Relevant training on computer systems, i.e. Framework i
* Safeguarding / child protection training

The SPA and MASH Team Manager is responsible for co-ordinating and directing MASH operations and ensuring that MASH team members carry out their respective roles so that the process runs smoothly and the main objectives of the MASH are met.

Issus relating to individuals MASH team members should be raised with their originating agency.

Also see section 7.

**DISPUTE RESOLUTION AND ESCALATION**

The protocol aims to provide the framework for multi-agency information sharing and practice that improves outcomes for children and families. In the event of any disagreement arising between partner agencies relating to MASH operations or decision-making, this will be dealt with in the first instance at the Multi Agency Safeguarding Hub level through discussion amongst partner team members.

Where a resolution cannot be found at this level, the matter should be raised in writing with the First Response Area Manager.

The First Response Area Manager will make a judgement on whether to:

* Try and resolve the dispute on the MASH level or
* To raise the issue with senior staff within the MASH partner agencies
* Bring the issue to the attention of the MASH Operation Group

**EVALUATION AND QUALITY ASSURANCE OF MASH**

* Each partner agency will be responsible for ensuring the quality and accuracy if information provided
* Agencies remain responsible for the professional conduct and quality of work of their staff working within the MASH and should take action to address any capability of disciplinary matters
* The Operational Protocol will be reviewed annually by the MASH Strategic Group and the Information Sharing Agreement and Information Sharing Guidance will be reviewed annually by KMIP.

**MANAGEMENT OF SPECIFIC ISSUES IN FIRST RESPONSE**

**Domestic Abuse Notifications (DAN’s)**

Current response to DANs

Single Point of Access receives Domestic Abuse Notification (DANs) from Kent Police. These are pre-screened by a Referral Information Officer (RIO).

DANs for children who are open to Children Services are screened by a RIO for any immediate safeguarding concerns. If immediate safeguarding concerns are identified the SPA and MASH Practice Manager reviews the notification alerting the allocated Area Social Worker and Practice Manager. The Notification is then recorded on Framework i as a significant contact and allocated to the Area Social Worker and Practice Manager.

If no immediate safeguarding concerns are identified the Notification is recorded on Framework i as a significant contact and allocated to the Area Social Worker and Practice Manager.

For children not currently open to Medway Children Services the notification is reviewed by the SPA and MASH Practice Manager.

High Risk DANs are RAG rated Red or Amber – if threshold is met on the information provided in the notification the SPA and MASH Practice Manager will progress the Contact and Referral to the Assessment Team.

If threshold is not met on the information provided within the notification the Contact and Referral is allocated to a MASH Social Worker.

Medium Risk and Standard DANs are reviewed by the SPA and MASH Practice Manager, information already held in relation to the children on Framework i will also be considered to inform a decision.

If threshold is not met for Children Services parents are provided with information about local domestic abuse services and the impact of domestic abuse on children and can be referred to Early Help or sign posted to other relevant services.

Aspiring response to DANs

Single Point of Access will triage the Standard and Medium Risk Police Domestic Abuse Notifications (DANs) along with representatives from Health, Education, Probation NPS, Probation CRC, Kent Police, Children Services and Early Help.

High Risk DANs will actioned by Children Services immediately.

The purpose of the meeting will be to share information, agree risk and what further actions are needed.

A pre triage daily meeting will be held with Kent Police, a Referral Information Officer from the SPA and an Early Help Co-ordinator. The pre triage meeting will identify the DANs of cases open to the Area Teams and the notification for unborn children under 16 weeks gestation.

The triage meeting will be held daily and Children Services, Kent Police, Education, Health and Early Help will review the notification to share information, agree risk and what further action is needed.

If threshold is met for Children Services the SPA and MASH Practice Manager in the SPA will progress the Contact and Referral and consideration will be given to a Child and Family assessment.

If threshold is not met consideration will be given to a referral to Early Help or for the education and/or health representative to update the child(ren) school and/or nursery and the allocated health professional so they can offer support.

Midwifery Safeguarding Meeting

The Midwifery Safeguarding Hub is a multi -agency meeting held once a month at Medway Maritime Hospital. The purpose of the meeting is to share information, explore what further actions are needed and agree if threshold is met for a referral to Children Services.

The meeting includes the SPA and MASH Team Manager and representatives from Midwifery including the Safeguarding Lead for Midwifery, Early Help Hub Manager, Health Visiting, Looked After Children Nurse and the Midwifery Mental Health Team.

The allocated community midwife gains consent from parents to gather and share information with other agencies. If threshold is met for a referral to Children Services the community midwife is tasked with making the referral following the meeting. If threshold is not met consideration is given to a referral to Early Help. Further actions can also been agreed by the members of the meeting for the community midwife to further explore.

The community midwife is responsible for keeping the parents informed of decisions and actions agreed at the meeting.

Missing Children from Home and Care

First Response oversees the case management of Missing Incidents of young people in Medway including children placed in Medway by other Local Authorities. Kent Police send missing and found compacts to Medway Children Services these are reviewed daily. Children open to Medway Children Services and children missing from home in Medway are all offered a return interview to explore the reasons for the missing incident and to implement actions to prevention a repeat missing incident.

Children placed in Medway by other Local Authorities are forwarded copies of the Police Compacts and are asked to provide First Response with a copy of their Return Interview.

The Missing and Exploitation Co-ordinator(Gangs, Children Sexual Exploitation and Missing Persons) also sits in First Response. The role includes maintaining a comprehensive overview of missing children and those vulnerable to and at risk of exploitation, identify those who are risk of significant harm, and assist alongside Area Teams to co-ordinate the response from internal departments and partners to reduce the likelihood of harm occurring to vulnerable children.

The role will also follow up with individual youth workers, and other Local Authorities when Return Home Interviews are not received in a timely manner. The role will also be responsible for collating themes and impact of any disruption activity.

No-Name Consultation Service

The aim of the No Name Consultation Service is to provide education professionals with advice on safeguarding issues and processes, such as to whether or not to make a referral, where concerns are held, over a child or young person.

When engaging in a consultation, no identification details for the child or family will be requested and therefore it is not required that parents/carers consent is given prior to the consultation.

The designated telephone number for the No Name Consultation Service is as follows: **01634 331662**

The service will be operational between the hours of 9.30am to 12.30pm Monday to Friday (excluding Bank Holidays). On calling the service, a Social Worker will be available to provide advice and guidance, offering a recommendation if necessary on the way to proceed. All the information given, during the consultation will be recorded ***(see Appendix A)*** and emailed to the person who has sought the consultation, within one working day, summarising the concerns and the recommendation/s provided. Should any information be recorded inaccurately, we ask the professional receiving the information to feed this back to First Response, Children’s Services to enable the corrections to be made.

If following the consultation, it is assessed that the threshold has been met for a referral to Children’s Services; the record of the consultation can be copied by the referrer into the contact and referral form, to aid the completion. Once the full contact and referral form is completed including consent being sought from parents (unless to do so would put child at risk of harm), the referrer will be submit to the Single Point of Access so that Children’s Services can respond accordingly.

Prior to seeking consultation First Response ask that professionals discuss their concern/query with the Designated Child Protection Lead/line manager for initial guidance.

Children’s Services will maintain a record of each consultation given any agreed recommendations, allocating a unique reference number to each consultation, for tracking and reviewing purposes.

First Response is also represented at the following panels:

Medway Youth Offending Risk Management Panel – the panel is held once a month by Medway YOS to share information and agree actions to reduce the risk of re offending and ensure safety and wellbeing.

Kent Police MCET Meeting – the SPA and MASH Team Manager attends the monthly MCET meeting to share and gain information about high risk children who are frequently going missing from home and care and therefore maybe deemed to be at risk of exploitation.

Missing and Exploitation Panel - The purpose of the panel is to share information and support the development of safety plans for young people in Medway considered to be experiencing exploitation (CSE, CCE, Gang involvement and Missing).



**Appendix 1**

**Appendix 2:**

**MASH Roles and Responsibilities**

**BROAD PURPOSE/CONTEXT**

Multi Agency Safeguarding Hubs (MASHs) co-locate key agencies and their data into a secure assessment, research and referral unit for notifications on vulnerable children and young people.

Agency partners in MASH will work as part of a dynamic multi-agency integrated team assessing notifications and referrals regarding children aged 0 – 18yrs.

The MASH process includes searching for and collating information from a range of sources including databases and other professionals. With due regard for confidentiality, the MASH professional is responsible for interpreting and sharing the information that is necessary to safeguard and promote the welfare of the child/young person.

MASH Role

**MAIN DUTIES AND RESPONSIBILITIES**

1. Maintain constructive relationships with a broad range of internal and external stakeholders and specifically with professionals from a range of disciplines in other Services.
2. Through liaison, dialogue and searching appropriate databases collect and collate relevant information to add to the multi-agency risk assessment.
3. Record, interpret and present information and issues that can impact on the risk or needs assessment of the child/young person. This may involve disclosing proportionate and relevant information related to the parents/carers, siblings or others in contact with the family.
4. Explain clearly, and with sound rationale, related safeguarding information to a wide range of professionals.
5. Participate in the MASH multiagency risk assessment to inform case management, advising where necessary and challenging decisions where appropriate.
6. Identify service gaps and issues relating to service pathways and/or cross boundary arrangements.
7. Escalate evidence of ineffective safeguarding arrangements within or outside the MASH.
8. Immediately report where issues require escalation or the case is likely to become subject to press or public interest.
9. Demonstrate through personal and professional example a commitment to equality of opportunity for all groups of staff and service users and challenge discrimination, racism, sexism and other forms of unjust behaviour.
10. In addition to the above Children’s Social Care is responsible completing the analysis of information gathered in the MASH episode and providing a recommendation to the SPA and MASH Practice Manager.

Individual role descriptors can be developed by home agencies to reflect individual requirements, building on the main duties and responsibilities described above.

**Appendix 3**

**MASH Partner Agency Profiles**

|  |
| --- |
| **Agency**: SPA (Single Point of Access) and MASH**Location**: Co-located**Staff profile:**1 x Team Manager3 x Practice Managers5 x Social workers5 Referral and Information Officers**Summary**The team is responsible for receiving all new contacts and referrals to Medway where there are concerns for the welfare of children. The Referral and Information Officers receive all telephone calls and electronic referrals from professionals and the public. The Practice Managers are responsible for screening all contacts and making a decision about which of these go through the MASH information gathering and analysis process. The SPA and MASH also co-ordinates daily MASH meetings. All information is recorded on Framework i. |
| **Agency:** Police**Location:** Co-located**Staff Profile:** 1 x DS (First Response)1 x Police staff –MASH Information Coordinator**Summary:**The Co-Located Police team aim to provide a swift response to all requests for those subjects who need to go through the detailed MASH process; these MASH cases are referred to Police through the agreed MASH process having been graded as Green, Amber or RED; depending on the perceived urgency and known risk level. Police utilise a variety of databases and systems to interrogate and assess risk as part of a MASH enquiry, after which after a detailed evaluation is disseminated back to Children's Services with all known research completed. The Police team endeavour to support all partners both those that are co-located and those who are virtual; by providing them with clear and comprehensive intelligence to Safeguard Children at the earliest opportunity.The DS (First Response) is the Agency Decision Maker regarding all Strategy Meetings relating to new referrals and will be part of the daily DAN (Domestic Abuse Notification) Triage and Op Encompass. |
| **Agency:** Education**Location:** Co-located**Staff Profile:** 1 x MASH Education Officer**Summary:** Officer is responsible for gathering information from an Education perspective on contact and referrals that have been accepted to go through the MASH process. Officer inputs information on Framework i. Officer responds to enquiries on Education related matters from other professionals, both within MASH and external. Officer advises schools on whether referrals are suitable and relevant. Officer also acts as the links between Education and schools. Officer contributes to MASH meetings.  |
| **Agency:** Youth Offending Service **Location:** Strood Youth Centre**Staff Profile:** Whole team - Lead responsibility lies with Practice Manager for YOS.**Summary:** The whole team support the MASH by undertaking the research as part of their Duty tasks. This is overseen by a duty manager and Group Leader. The YOS have responsibility for all young children who are classified Medway residents and are known to the Youth Criminal Justice system, either Pre-Court or Post sentence. The YOS has responsibility for the management of Court Orders, Pre Court disposals and early intervention including Anti-social behaviour. The Youth Crime Prevention Panel offers dedicated support to young people identified through universal services or specialist agencies as being at risk of becoming involved in crime or Anti-social behaviour. The YOS is made up of a multi-disciplinary group of professionals including health, social workers, police and Probation.  |
| **Agency:** Health **Location:** Co-located**Staff profile:** 1 X MASH Health Professionals **Summary:** The MASH process includes searching for and collating health information from a range of NHS providers both locally and further afield. With due regard to patient confidentiality, the MASH health professional will interpret and share the information that is necessary to safeguard and/or promote the welfare of a child. The MASH Health Professional will be expected to contribute to a multi-agency analysis of risk on a case by case basis to help to inform the case management, advising where necessary and challenging decisions when appropriate.Specifically the role and responsibilities include:To adhere to the MASH Information Sharing protocolTo contribute to decision making by collating and analysing relevant health information using the Strengthening Families FrameworkTo use professional judgement as to which health agencies to approach for information in relation to individual requests but will routinely request information from GP and MFTTo form analysis based on information gathered and provide indication of the outcome in accordance with the Threshold DocumentTo contribute to discussions around outcomes of MASH referralsTo challenge decisions where there is a disagreement over the application of threshold and to raise in line with MSCB Escalation PolicyTo document MASH information in a timely way on relevant systems and health MASH databaseTo liaise with relevant health professionals with regards to outcomes and actionsTo flag where agencies are not sharing information in a timely wayTo participate in MASH team meetings and group supervision |
| **Agency:** Housing **Location:** Homeless Prevention and Assessment Team, Kingsley House**Staff profile:** Whole team via duty service- Operational Lead responsibility lies with Principal Housing and Review Manager.**Summary:**The Homeless Prevention and Assessment Team offer a range of advice and support to those that have a housing need. The service provides advice and assistance to people that find themselves homeless or rough sleeping as well as rehousing those whose existing properties may no longer be suitable. The service offers support to improve the standard of accommodation within the private sector including the adaptation of existing properties for those that may have a disability.  |
| **Agency:** Early Help **Location:** Co-located**Staff profile**: Early Help Social Worker – co-located in SPA Early Help Co-ordinator – co-located in MASHEarly Help Domestic Abuse – co-located in MASH Monday – Wednesday mornings (plan to recruit full time post)**Summary:**The Early Help Social Worker is the decision maker for all Early Help Requests either from a contact or outcome from MASH enquiry. The Early Help Social Worker will decide whether threshold is met and level of presenting need requires an Early Help Service. The Early Help Social Worker will also decide on the most appropriate type of Early Help Service to offer the family i.e. level 3/level 2.The Early Help Co-ordinator will undertake all MASH enquiries and is able to feedback about families that may be accessing services within the Children and Family Hubs and Early Help Services. Early Help Domestic Abuse worker will be based in MASH to contribute to any MASH discussions and participate in the DAN Triage when this goes live. |
| **Agency:** 0-25 SEND **Location:** Co located **Staff Profile**: 0-25 SEND Social Worker**Summary:** The 0-25 Disability Social Worker, is an experienced Specialist Social Worker who has a range of information, knowledge and skills about disabilities and services in Medway and has an understanding about the law and policy which governs and guides the delivery of our intervention. The specialism is largely gained from working with children, young people and adults who have severe and profound disabilities. There are two social workers on duty each day, one of which is based in MASH. Their role is to contribute their knowledge and expertise on MASH enquiries where there is a child in the family with a disability and provide additional oversight, swifter allocation and timely access to service provision. |
| **Agency:** NPS Probation**Location:** Kroner House, Ashford**Staff Profile:** Probation Officer**Summary:** NPS Medway have an identified single Point of Contact who is a qualified Probation Officer based in the Medway Team who is supported by a 1.0fte Case Administrator based at the Central Referral Unit who has access to Framework i.   The role will be the conduit linking Medway MASH to Medway Probation Officers and Probation Service Officers (known as Offender Managers) who are working with statutory cases (adults).  All Domestic Abuse Notifications (DANs) for Medway will be managed by the Case Administrator based at the Central Referral Unit via the NPS Kent safeguarding inbox. Data will be collated on both the numbers of Medway DAN’s received and the number of agency involvement requests made by Medway MASH.  This data will be reported to the appropriate Board. |
| **Agency:** Turning Point**Location:** High Street Chatham**Staff Profile:** Duty Worker**Summary:** Turning Point provides services for anyone who is affected by drugs or alcohol and offers a range of integrated substance misuse services to support recovery. The role will be the link between Turning Point Services and Medway MASH. |
| **Agency:** Children’s Social Care - Missing and Exploitation**Location:** Co-located**Staff Profile:** Missing and Exploitation Co-ordinator (Gangs, Children Sexual Exploitation and Missing Persons)**Summary:** The purpose of the role is to maintain a comprehensive overview of missing children and those vulnerable to and at risk of exploitation within Medway in order to identify those who are risk of significant harm, assisting alongside Area Teams to co-ordinate the response from internal departments and partners to reduce the likelihood of harm occurring to vulnerable children.The role will also follow up with individual youth workers, and other Local Authorities when Return Home Interviews are not received in a timely manner. The role will also be responsible for collating themes and impact of any disruption activity. |

**Appendix 4**

**Information Sharing Agreement**

**KENT & MEDWAY INFORMATION SHARING AGREEMENT**

Sharing of information is crucial to the successful delivery of local services. This Information Sharing Agreement provides a framework to enable a number of organisations and public bodies across Kent and Medway to share personal information.

This Agreement provides for openness and transparency in information sharing, as well as appropriate governance and support, in order to assist signatory organisations and public bodies to share personal information lawfully, safely and securely.

This Agreement reflects the requirements of the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA 2018). The GDPR aims to refocus data protection to remind us that it is people who are at the heart of the process; people whose personal information matters to them. It therefore gives people rights in relation to their information, and also requires organisations and public bodies to operate in a fair, lawful and transparent manner when they, for example, obtain and collect; use, share and publish; store, archive and delete people’s personal information.

But the GDPR also specifically recognises that “data protection” should not be an excuse to prevent proper sharing of personal data. It reminds us that we can (and sometimes we have a legal obligation to) share personal information. Information sharing can be vital, for example in emergency situations. We are enabled to share such information, and protected by the law when we do, so long as:

* we have proper reasons to share and use personal information, and we share only the information relevant to and adequate for those purposes;
* we tell individuals why and how we will share their information, including identifying for them (and for ourselves) the lawful basis for sharing the information;
* we ensure that the personal information is factually accurate;
* we store personal information for the minimum time necessary for the purposes for which the information was obtained;
* we take practical steps to prevent loss of or damage to the personal information; and
* we adopt good governance and record keeping procedures concerning our use of personal information.

This Agreement addresses each of those bullet points below. It enables its signatory organisations and signatory public bodies to comply with the requirements of the GDPR and the DPA 2018.

Signatory organisations to the Agreement automatically become members of the Kent & Medway Information Partnership (K-MIP). More information is available on [Kent Connects](https://fs.klz.org.uk/adfs/ls?version=1.0&action=signin&realm=urn%3AAppProxy%3Acom&appRealm=3c3b1b19-418e-e711-941b-001018f502cb&returnUrl=https%3A%2F%2Fportals.kentconnects.gov.uk%2F&client-request-id=78611EBB-CE54-0000-D49D-707854CED301), which operates as the K-MIP web portal. K-MIP will hold quarterly meetings and will review this Agreement annually.

**Version Control**

|  |
| --- |
| **Document filename:**  |
| **Programme** | K-MIP | **Project** | GDPR |
| **Version issue date** | [Publish Date] | **Version** | 1 |

**Data Protection Officers**

All public authorities (i.e. bodies subject to the Freedom of Information Act 2000 or specified by the Secretary of State in regulations) are required to appoint a Data Protection Officer (“**DPO**”). DPOs perform an independent role, governed by the GDPR, overseeing, facilitating and promoting data protection within their organisations. It is also good practice for non-public authorities who carry out public tasks to appoint a DPO.

Some other bodies are also required to appoint a DPO:

1. where the key operations of the organisation involve regular tracking and profiling of individuals via large volumes of personal information or via personal information held for a long time or covering a large geographical area (for example, tracking individuals’ movements through the GPS in their vehicles);
2. where the key operations of the organisation involve processing of large volumes of special category personal information (for example, processing of health data by a hospital) or information concerning criminal convictions and offences.

**IG Contacts and SIROs**

Not all organisations will have a DPO. But all organisations will have an individual who is tasked with responsibility for information governance or for protecting personal information or strengthening information assurance. These individuals are often called Information Governance contacts or Senior Information Risk Owners (SIROs).

A list of the DPOs, IG contacts or SIROs of signatories to this Agreement can be found here, on the K-MIP portal.

1. **Information to be shared**
* We recognise that this Agreement concerns “personal information”. That means any information relating to an identified or identifiable living individual.
* We recognise that information relating to “legal persons”, such as companies or corporate entities, is excluded from the definition of personal information (but of course the information of all their living employees is “personal information”). The information of people who have passed away is not “personal information”, but we may still need to treat it confidentially (for example, as a result of the Code of Practice for the NHS).
* We accept that “personal information” is broadly defined:
	+ An individual may be identifiable directly or indirectly;
	+ In particular, an individual may be identifiable by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living individual;
	+ Such information can include photographs and other recorded images, CCTV and voice recordings;
	+ Information which is also in the public domain (for example, information on social media or otherwise published online or in physical form) remains “personal information” if it identifies a living individual;
	+ Expressions of opinion about individuals are their personal information, as is the factual basis for the opinion.
* Sometimes we will share **special category personal information**, which is defined as only the following types of information:
	+ the **racial** or **ethnic** origin of the individual,
	+ his/her **political** opinions,
	+ his/her **religious** or **philosophical** beliefs,
	+ his/her **health,**
	+ his/her **sex life** and **sexual orientation**
	+ whether he/she is a member of a **trade union**,
	+ the processing of **genetic data**,
	+ the processing of **biometric data** in order to uniquely identify a person (“biometric data” is information relating to individuals’ physical or behavioural characteristics which allow unique identification of that individual, such as fingerprint recognition, voice recognition, facial recognition or walking pattern recognition).
* We recognise that personal information concerning criminal convictions and offences is not special category personal data, but is a very sensitive type of personal information which can only be shared in narrow circumstances.
* We will share the personal information of our service users, where it is fair and lawful to do so and where that sharing takes place in a transparent manner. These elements – fairness, lawfulness and transparency – are reflected in our privacy notices (or fair processing notices or data protection notices) and our privacy policies or data protection policies.
* **Pseudonymisation:** Sometimes we will be able to “pseudonymise” the information we share. Pseudonymisation substitutes the identity of the individual in such a way that additional information is required to re-identify that individual.
	+ Pseudonymisation is not anonymisation. Anonymisation irreversibly destroys any way of identifying the individual, usually by scrubbing all identifying information held by an organisation.
	+ Instead, pseudonymisation means “key coding” the information or masking the identities of individuals, for example by using random characters instead of names. The organisation then holds the pseudonymised information completely separately from the information that identifies the individual.
	+ Pseudonymisation limits the ability of a recipient to attribute the information to a specific living individual.
	+ We recognise that pseudonymised information remains personal information, and so sharing it must be fair, lawful and transparent. But the pseudonymisation means we can use that information for more purposes and can keep it for longer than non-pseudonymised information.
	+ We acknowledge that it is good practice to consider whether personal information can be pseudonymised before it is shared and to take every opportunity to pseudonymise where possible.
1. **Purposes for sharing personal information**
* We recognise that there is a wide array of purposes for which we could share personal information. However, whenever we share personal information, we have to have a **specified, explicit and legitimate purpose** for that sharing. This means that the reason(s) for each instance of sharing of personal information will be set out, clearly and understandably, in our privacy notices (or fair processing notices or data protection notices), so that individuals will appreciate why their personal information may be shared.
* We recognise that:
	+ The organisation or public body providing/disclosing the personal information must have a specified, explicit and legitimate purpose for each instance of providing or disclosing the information;
	+ The organisation or public body receiving/collecting the personal information must have a specified, explicit and legitimate purpose for each instance of receiving or collecting the information.
* Our purposes for sharing personal data will be specified and made explicit in our privacy policies or data protection policies and our privacy notices (or fair processing notices or data protection notices), which will be provided to the individuals whose personal data is shared (see section 5 below).
* We recognise that it is important for us to agree the types of purposes for which it is legitimate for us to share personal information. We may share information for the following legitimate purposes:
	+ To provide direct health or social care to individuals, including mental healthcare;
	+ To maximise individuals’ access to benefits;
	+ To support individuals in, or into, employment;
	+ To assist individuals with housing and enforce housing standards;
	+ To support individuals who are homeless;
	+ For reasons of environmental protection;
	+ To help individuals who have been identified as at risk, or who may be so identified;
	+ To address fuel poverty and water poverty;
	+ To provide counselling services;
	+ To safeguard vulnerable adults;
	+ To support vulnerable families;
	+ To safeguard children and young people;
	+ To support or improve educational provision;
	+ To detect, prevent or provide assistance in cases of domestic abuse;
	+ To enforce professional standards;
	+ To support the Prevent Strategy;
	+ To aid with the detection or prevention of crime;
	+ To support Liaison and Diversion Schemes;
	+ For reasons related to the detection and prevention of terrorism;
	+ To aid with the detection and prevention of non-criminal acts that are nevertheless unlawful;
	+ To address anti-social behaviour;
	+ To support release from custodial settings;
	+ To improve the efficiency of service provision;
	+ To improve operational efficiency;
	+ For reasons of public safety and emergency planning;
	+ To assist emergency responders;
	+ For research purposes;
	+ To calculate and levy tax and to investigate matters relating to tax;
	+ To combat fraud;
	+ For purposes of immigration control;
	+ For purposes related to inquests or investigations by Coroners;
	+ To facilitate reimbursement of costs or to apply charges for services.
* We recognise that the type and extent of personal information which it is fair and lawful to share will be different for each of the purposes set out above.
* We will never use any personal information shared with us for a purpose that conflicts with or is not compatible with the purpose(s) for which it was shared.
1. **Fair sharing**
* We recognise that all our handling of personal information, including sharing that information, must be fair. Fairness is at the core of our obligations to individuals.
* We will ensure that, whenever we share personal information, we will do so fairly. This means:
	+ We will never deceive individuals as to how we will use their information, and in particular will never deceive them about whether, how or with whom their information may be shared.
	+ We will ensure that individuals have realistic expectations about how we will use and share their information. We will set these expectations by being transparent about how we use and share information (more in section 5 below).
	+ We will always consider the impact on the individual of sharing their information and whether that impact is justified by the reason we have to share the information.
	+ We will take care when we share opinions about individuals and will make sure there is a proper evidential basis for the opinions. If sharing the opinion would have a potentially detrimental effect on the individual, then we will only share that opinion where the reason for sharing outweighs any detriment that the individual will suffer.
1. **Lawful bases for sharing**
* We recognise that we are required to identify a lawful basis for each instance of sharing personal information.
	+ We only need to identify one of the lawful bases set out below to justify the sharing of personal information, but we can rely on more than one basis.
	+ We will record in our Record of Sharing (see section 9 below) the lawful base(s) on which we are sharing information and justify our reliance on it/them.
* In many instances, the lawful basis will be that the sharing of the personal data is required for the performance of a public task. This takes two forms:
	+ The sharing necessary because we are **carrying out a specific task in the public interest** (e.g. providing family support services), where the task is laid down by the law (i.e. the overall task is contained in a statute, regulation, statutory guidance or laid down by case law); or
	+ The sharing is necessary because we are **exercising our own official authority** (e.g. fulfilling our duties, carrying out our functions or exercising our powers), where that authority is laid down by the law (i.e. the overall authority is contained in a statute, regulation, statutory guidance or laid down by case law).
* We accept that, in order to rely on the public task lawful basis, the sharing must be strictly required in order for us to perform the relevant public task. This means that if a less privacy invasive course than sharing personal information is available then we should adopt the less invasive course.
* We can share personal information where that is necessary in order for us **to comply with a legal obligation** to which we are subject.
	+ This does not mean that there must be a legal obligation specifically requiring the sharing, but our overall purpose must be to comply with a legal obligation.
	+ We recognise that, to rely on this basis, we must be bound by the legal obligation. It is not enough to have a legal power. If we have discretion about whether to share the personal information, we must consider whether we can rely on the public task basis.
	+ Contractual obligations do not qualify as a legal obligation for these purposes.
* We can share personal information where it is necessary in emergency situations or where the **vital interests** of the individual or another living person need to be protected.
	+ “Vital interests” include protecting the life of a person, or protecting their bodily integrity. This is limited in scope and applies, for example, to life or death situations, or to contending with infectious diseases or humanitarian emergencies.
* We can share personal information where that sharing is necessary for the **performance of a contract** with the relevant individual(s) or to take steps at the request of the individual(s) before entering into a contract.
* In some limited circumstances, we can share personal information for **legitimate interests**, which means we are happy to take full responsibility for justifying the sharing because we are confident that we are protecting the interests of the individual(s) or we are acting in our own specific and compelling interests or in the specific and compelling interests of a third party.
	+ We recognise that to rely on this basis, we have to consider the potential impact on the individual(s) of sharing the personal data. This includes social or economic disadvantage; risk of physical or financial damage; inability of the individual(s) to exercise their rights (including data protection rights). Importantly, we recognise that the interests of the individual(s) could override the interests we are trying to protect, which means we cannot rely on this as a basis for sharing the information. This could happen, in particular, if the personal information is being shared in ways the individual(s) do not reasonably expect, unless there is a compelling reason which justifies the sharing.
	+ We must make sure we give particular weight to protecting children’s personal information.
	+ If there is another less intrusive way to achieve the same result, then we cannot rely on this basis.
	+ If we are not public authorities, then we can rely on this basis so long as the elements above are complied with.
	+ If we are public authorities, then we cannot rely on this basis for any sharing of personal information which is part of the performance of our public tasks. However, we can consider this basis where the sharing of personal information is happening as a result of other legitimate purposes outside of our public tasks. It is generally preferable for public authorities to avoid this basis, so the circumstances where we can rely on it to share personal information will be very limited.
* **Consent:** we recognise that there are many myths around the need for the individual to consent to the sharing of their personal information. The GDPR and the DPA 2018 have changed the requirements concerningconsent. This means that:
	+ We **will not** seek an individual’s consent to share their personal information where it is not possible for that consent to be withheld or withdrawn – i.e. where we would rely on one of the other lawful bases to share the information even if the individual withheld their consent or withdrew it. We must not trick individuals into thinking that they can refuse to consent to the sharing of their personal data when that is not correct.
	+ We **will not** seek an individual’s consent to share their personal information where there is a power imbalance between us and the individual, for example where the individual is vulnerable or is reliant on us for the provision of services.
	+ We will therefore only rarely use consent as a lawful basis for sharing personal information, and will only use it where we want to give individuals the ongoing power to decide whether their information is shared or not.
* When we are **sharing special category personal data**, we recognise we have to identify **both** a lawful basis from one of those set out above, and a further condition from the list below on which we can rely to justify the sharing:
	+ the sharing is necessary for the purposes ofcarrying out our obligations and exercising specific rights in the field of employment and social security and social protection law; or
	+ the sharing is necessary for health or social care purposes;or
	+ the sharing is necessary for reasons of public interest in the area of public health, and is carried out under the responsibility of a health professional or another person who owes the individual a duty of confidentiality; or
	+ the sharing is necessary for archiving purposes, scientific or historical research purposes or statistical purposes and is in the public interest; or
	+ the sharing is necessary for the exercise of a function conferred on us by an enactment; or
	+ the sharing relates to personal information which are manifestly made public by the individual; or
	+ the sharing is necessary for the establishment, exercise or defence of legal claims; or
	+ the sharing is necessary for reasons of substantial public interest , and we have an appropriate policy document in place (i.e. a policy document that is reviewed regularly and explains how we will comply with the data protection principles and our policies for retention and erasure of personal information), and one of the following conditions applies:
		- the sharing is necessary for the exercise of a function conferred by an enactment; or
		- the sharing is necessary for the administration of justice; or
		- the sharing is necessary for equal treatment monitoring; or
		- the sharing is necessary to prevent or detect unlawful acts, including an unlawful failure to act; or
		- the sharing is necessary to protect the public against dishonesty, malpractice or other serious improper conduct; or
		- the sharing is necessary to prevent fraud; or
		- the sharing is necessary for certain disclosures made under the Terrorism Act 2000 and the Proceeds of Crime Act 2002; or
		- the sharing is necessary for the provision of confidential counselling, advice or support services.
* In limited situations, we can share special category personal information where the individual has given their explicit consent to the sharing. This will not often be a proper basis for sharing special category personal information, but may apply, for example, where an individual consents to the use of their detailed health information, non-pseudonymised, for research purposes.
* We accept that we cannot share **personal information concerning criminal convictions and offences** unless we can rely on one of the following bases:
	+ the sharing is necessary to protect the vital interests of an individual (as above, this means to protect the life or physical integrity of an individual); or
	+ the sharing is necessary for (i) any legal proceedings; (ii) obtaining legal advice; or (iii) establishing, exercising or defending legal rights; or
	+ the sharing is necessary for reasons of substantial public interest, and we have an appropriate policy document in place, and one of the conditions below applies:
		- the sharing is necessary for the exercise of a function conferred by an enactment; or
		- the sharing is necessary for the administration of justice; or
		- the sharing is necessary for preventing or detecting unlawful acts; or
		- the sharing is necessary for equal treatment monitoring; or
		- the sharing is necessary to prevent or detect unlawful acts, including an unlawful failure to act; or
		- the sharing is necessary to protect the public against dishonesty; or malpractice or other serious improper conduct; or
		- the sharing is necessary to prevent fraud; or
		- the sharing is necessary for certain disclosures made under the Terrorism Act 2000 and the Proceeds of Crime Act 2002; or
		- the sharing is necessary for the provision of confidential counselling, advice or support services.
	+ We recognise that an “appropriate policy document” will explain how we will comply with the data protection principles; will explain our policies for retention and erasure of personal information and that the policy documents will be reviewed regularly.
1. **Privacy Notices - Transparency of sharing personal information**
* We recognise that being transparent about how we use and share personal information is key to engendering trust in the processes which affect individuals.
* We will therefore ensure that we tell individuals about how their information will be shared by providing those individuals with clear, concise and easily understandable privacy notices (or fair processing notices or data protection notices).
	+ Where we are sharing personal information of individuals who are vulnerable, including people with disabilities or people who have difficulties accessing information, we will ensure that our privacy notices (or fair processing notices or data protection notices) are written and provided in a way that is accessible to and understandable by those individuals.
	+ Where we are sharing personal information of children, we will ensure that our privacy notices (or fair processing notices or data protection notices) are written in child friendly language.
* We acknowledge how important it is for the proper operation of this Agreement that our privacy notices (or fair processing notices or data protection notices) are robust, and so will ensure that they all comply with the Information Commissioner’s Privacy Notices Code of Practice.
* We will ensure that our privacy notices (or fair processing notices or data protection notices) are explicit about how and why personal information will be shared with signatories under this Agreement.
1. **Individuals requesting information**
* We will treat any request for a requester’s own information as a Subject Access Request.
	+ We will usually respond to Subject Access Requests under our own processes, which we will ensure comply with the Information Commissioner’s Subject Access Code of Practice.
	+ We recognise that in some narrow situations, the signatories to this Agreement will be “joint controllers” – i.e. they will decide together all the purposes for using the personal information that they share, and they will decide together the broad ways in which that personal information will be used. Where we are joint controllers, we will ensure that we have an arrangement that clearly delineates our respective responsibilities, including who will handle and respond to Subject Access Requests.
* Any information held by a public authority (as designated under the Freedom of Information Act 2000, “FOIA”) may fall within a FOIA request. Organisations who are not FOIA public authorities recognise that information shared under this Agreement may have to be disclosed under FOIA.
1. **Rights of the people whose personal information we share**
* We acknowledge that we will need to work together to ensure that the individuals whose information we share can exercise their data protection rights.
* **Right of subject access**: this is addressed in section 6 above.
* **Right to rectification:** An individual has a right to ask us to correct inaccurate personal information about them, or complete that information if it is incomplete. Personal information is inaccurate if it is incorrect or misleading as to any matter of fact. If we decide that we must correct any inaccurate information, or complete any incomplete information, then we have to take further steps if we have shared the inaccurate or incomplete information under this Agreement.
	+ We must contact each recipient of the inaccurate or incomplete information and inform them of the correction or completion we have made, unless this proves impossible or involves disproportionate effort.
		- “Impossible” is an all or nothing situation, and we must be able to demonstrate the factors that actually prevent us from informing each recipient.
		- “Disproportionate effort” is not the same as “inconvenience”. The more serious the potential impact on the individual arising from the future use by the recipients of the inaccurate or incomplete information, the less likely that our efforts to contact recipients will be “disproportionate”.
	+ If the individual asks us, we must also tell that individual who the inaccurate or incomplete information was shared with.
* **Right to erasure**: An individual has a right to ask us to erase personal information about them if certain limited circumstances apply. If we decide that we must erase any personal information pursuant to a request from an individual, then we have to take further steps if we have shared that information under this Agreement.
	+ We must contact each recipient of the information and inform them of the erasure, unless this proves impossible or involves disproportionate effort.
		- “Impossible” is an all or nothing situation, and we must be able to demonstrate the factors that actually prevent us from informing each recipient.
		- “Disproportionate effort” is not the same as “inconvenience”. The more serious the potential impact on the individual arising from the future use by the recipients of the information that we have erased, the less likely that our efforts to contact recipients will be “disproportionate”.
* **Right to restriction**: An individual has a right to ask us to restrict or suppress their personal information if certain limited circumstances apply. If we decide that we must restrict or suppress any personal information, then we have to take further steps if we have shared that information under this Agreement.
	+ We must contact each recipient of the information we have restricted or suppressed and inform them of the restriction or suppression, unless this proves impossible or involves disproportionate effort.
		- “Impossible” is an all or nothing situation, and we must be able to demonstrate the factors that actually prevent us from informing each recipient.
		- “Disproportionate effort” is not the same as “inconvenience”. The more serious the potential impact on the individual arising from the future use by the recipients of the information we have restricted or suppressed, the less likely that our efforts to contact recipients will be “disproportionate”.
	+ If the individual asks us, we must also tell that individual who the restricted or suppressed information was shared with.
* **Other rights:** We acknowledge that there are other rights of individuals: the right to object to processing of their personal information; the right to withdraw any consent at any time; the right of data portability; the right not to be subject to a decision based solely on automated profiling. We will ensure that we have processes in place to allow individuals to exercise these rights.
1. **Exemptions**
* We recognise that the DPA 2018 sets out a number of exemptions, which allow us to share information without needing to identify a lawful basis for the sharing and without needing to provide information to individuals about the sharing.
* We acknowledge that these exemptions must be narrowly construed, so that only the minimum sharing necessary is permitted.
* The exemptions are:
	+ the sharing is necessary for the purposes of preventing or detecting crime, the apprehension or prosecutors of offenders or the assessment of tax or duty;
	+ the sharing is necessary for the purposes of maintaining effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control;
	+ the sharing is required by an enactment, rule of law or court/tribunal order;
	+ the sharing is necessary for the purposes of actual or prospective legal proceedings, or obtaining of legal advice or establishing, exercising or defending legal rights;
	+ the sharing is necessary for discharging our functions protecting the public in relation to financial loss, harm by persons authorised to carry on any profession or other activity;
	+ the sharing is necessary for discharging our functions protecting charities and community interest companies and their property from mishandling;
	+ the sharing is necessary for discharging our functions protecting the public from maladministration and failures by a public body;
	+ the sharing is necessary for discharging our functions regulating anti-competitive behaviour;
	+ the sharing is necessary because we are discharging specific regulatory functions relating to legal services, the health service and children’s services (but are not related to our own complaints handling functions).
* If we are relying on any exemption(s) in order to share information, we must identify which exemption(s) and justify our reliance on them. We will do this on the Record of Sharing (see section 9 below).
* If we are unsure whether an exemption applies allowing us to share personal information, then we will escalate the matter by asking for advice from our DPO or from a senior officer within our organisation who has expertise in data protection.
1. **K-MIP Record of Sharing**
* We will ensure that we have a record of all information shared under this Agreement. As appropriate, we will complete a K-MIP One-Off Sharing Record or a K-MIP Repeat Sharing Record. We recognise the importance of keeping such records up to date.
* If we are sharing personal information under this Agreement in reliance on the public service delivery, debt or fraud powers in the Digital Economy Act 2017, then we will develop and agree a business case with the other organisations with whom we will be sharing information, in line with the Information Sharing Code of Practice: Public Service Delivery, Debt and Fraud.
1. **Sharing and keeping personal information securely**
* We will each compile an Information Asset Register, which identifies as a minimum:
	+ the information that we hold,
	+ where it is held and who is responsible for the information,
	+ how much information is held and whether any of it is personal information or special category personal information,
	+ who has access to the information,
	+ who is responsible for the information,
	+ whether the information is shared and, if so, with whom,
	+ the risks relating to the information and what the impact would be if those risks materialised.
* We will each maintain a record of our processing activities (ROPA), which shall contain as a minimum the following information:
	+ our name and contact details, the name and contact details of our data protection officer (where applicable) and the names and contact details of any joint controllers (where applicable);
	+ the purposes of our processing;
	+ a description of the categories of individuals and of the categories of personal information we hold;
	+ the categories of recipients to whom the personal information have been or will be disclosed including recipients in third countries or international organisations;
	+ where applicable, transfers of personal information to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers which are necessary for the performance of a contract with the individual, the documentation of appropriate safeguards;
	+ where possible, the envisaged time limits for erasure of the different categories of personal information;
	+ where possible, a general description of the technical and organisational security measures taken to ensure the security of processing.
* We will ensure that our employees are able to access only the shared personal information necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to personal information.
* We will ensure we maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.
* We will protect the physical security of the shared information. This means we will, as a minimum:
	+ Ensure our organisation controls physical access to its premises;
	+ Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises;
	+ Ensure proper physical control of printers and photocopiers so that personal information is not left lying on the printer/photocopier;
	+ Ensure secure disposal of printed materials, so that materials intended for disposal do not sit around in piles. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises;
	+ Ensure that old computers, printers and other electronic equipment is disposed of safely and that all personal information is irretrievably scrubbed from any memory before disposal.
* We will protect the electronic security of the shared information. This means we will, as a minimum:
	+ Ensure our organisation has a strong password policy that is adhered to by all staff members. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members;
	+ Ensure our organisation installs security patches on electronic devices (including ensuring all operating systems’ updates are installed in line with best practice);
	+ Ensure staff are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work;
	+ Ensure that any Wi-Fi connections are secure and that any guest Wi-Fi is on a segregated system, so that guests cannot access our systems from that Wi-Fi;
	+ Ensure that any information that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice;
	+ Ensure that our organisation complies with the best practice of cyber security as detailed by the National Cyber Security Centre.
* **Encryption:** We must ensure that all information held on portable devices, including laptops, tablets and USB/portable drives, has full disk encryption. This must be to industry standard, and as a minimum:
	+ FIPS 140-2/256 bit asymmetrical encryption; or
	+ CBC-AES 256-bit encryption.

A recognised mark of excellence in encryption is CCTM government accreditation (for more information, see the National Cyber Security Centre website).

* We will only e-mail special category personal information and information about criminal convictions or offences via secure e-mail.
* We have contracts and systems in place to ensure that any contractors and sub-contractors managing any aspect of data security are fully aware of and abide by this Agreement.
* We must not pass on or sell the personal information we obtain under this Agreement to other parties or organisations not party to this Agreement
* **Reporting a Breach**: We must have robust data breach reporting policies in place, and adhere to them, so that all personal data breaches are reported immediately when we become aware of the breach.
	+ A “personal data breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information which we have transmitted or stored or processed.
	+ If the personal data breach occurred in the course of information being shared under this Agreement, then the organisation/public body who discovers the breach must immediately inform the other organisations/public bodies involved in the sharing of the personal information. The organisations/public bodies involved will decide who will take the lead on addressing the breach and on whether the breach needs to be reported to the Information Commissioner or to the individuals concerned (which must happen without undue delay and usually within 72 hours of having become aware of the breach).
	+ Personal data breaches will be an open agenda item at all K-MIP quarterly meetings.
1. **Storing and deleting personal information**
* We recognise that one of the most important data protection obligations is that we limit the storage of personal information. We must only store information in a form that identifies individuals for as long as is necessary for the purposes for which we are processing the personal data.
* We must each have and implement comprehensive retention schedules, which:
	+ Set out the minimum necessary period of storage for different categories of personal information, which are determined taking into account:
		- The types of personal information that we process (organised, for example, by function);
		- The purposes for processing the personal information;
		- Why each type of personal information should be retained;
		- Any relevant industry standards or guidance;
		- Any relevant legal obligations to retain personal information for specific periods of time.
	+ Set out where the personal information will be stored and how it will be kept secure during the retention periods.
	+ Set out how any processors who process information on our behalf will comply with out retention periods.
	+ Set out how data will be archived or destroyed.
* We will have systems in place to adhere to the periods in our Retention Schedules and to review our Retention Schedules regularly. We will train our staff so that they are empowered to comply with our Retention Schedules.
* We recognise that the need to have and comply with Retention Schedules is not an excuse to dispose of personal information when it is still necessary for us to retain that information in order for us to provide services to individuals.
* Sometimes organisations are disbanded or are replaced by successor organisations.
	+ If one of our signatory organisations is disbanded, it will ensure that the personal information held by it is disposed of securely and confidentially;
	+ If one of our signatory organisations is replaced by a successor organisation, it will ensure that the personal information held by it is properly transferred to its successor organisation, subject to the successor organisation becoming a signatory to this Agreement. If the successor does not wish to become a signatory to this Agreement, the personal information will be disposed of securely and confidentially.
1. **Ensuring the personal information is accurate**
* We acknowledge that we have a general duty to ensure that personal information is accurate, which is separate from the requirement to take steps where an individual exercises the right to rectification. We will therefore have systems in place to identify any personal information that is inaccurate as to any matter of fact.
* If we discover that personal information is inaccurate as to any matter of fact, we will ensure that the information is made accurate and we will notify any signatory organisations or public bodies with whom we have shared that personal information of the accurate information.
* If we are notified that inaccurate personal information has been shared with us, we will immediately take steps to amend the inaccurate information.
* We acknowledge that opinions are accurate so long as they are correctly recorded. If we discover that an opinion is incorrect (for example because it is based on inaccurate information), then we will record that the opinion is incorrect. We recognise it may still be important to retain the incorrect opinion rather than delete it (for example, to explain why we took specific steps or in case of a complaint or a legal claim), but if retaining the incorrect opinion may harm the individual then we will delete the opinion.
* If we discover that we have shared an opinion which is incorrect because it is based on inaccurate personal information, we will notify any signatory organisations or public bodies within whom we have shared the incorrect opinion.
* If we are notified that an incorrect opinion has been shared with us, we will immediately take steps to delete the incorrect opinion, unless it is important to retain a record of that opinion. If so, we will ensure that the record clearly shows the opinion is incorrect.
1. **Sharing Information**
* We acknowledge that, when we become signatories to this Agreement, we will be expected to share personal information with other signatories in accordance with the provisions of this Agreement. We recognise that there should not be any need for signatories to enter into sub-agreements with each other in order to share personal information.
* We acknowledge that we will be required to enter into other information sharing agreements when we share personal information with organisations outside Kent and Medway, or with national organisations. We will make every effort to ensure, so far as practicable, that those agreements do not conflict with the requirements of this Agreement.
1. **Joining or withdrawing from this Agreement**
* We have published a list of current signatories to this Agreement on the Kent Connects portal.
* We invite organisations or public bodies who would like to join this Agreement to email or write to the K-MIP Chairman to express their interest in joining [see the [K-MIP portal](https://fs.klz.org.uk/adfs/ls?version=1.0&action=signin&realm=urn%3AAppProxy%3Acom&appRealm=3c3b1b19-418e-e711-941b-001018f502cb&returnUrl=https%3A%2F%2Fportals.kentconnects.gov.uk%2F&client-request-id=78611EBB-CE54-0000-D49D-707854CED301) for contact details].
	+ Where an organisation that is not a public authority wishes to sign this Agreement, they will be asked to declare all potential conflicts of interest, for example from other work they do for public authorities or their own commercial interests.
		- We will consider these potential conflicts of interest before sharing any information.
		- If any conflicts arise, we will determine whether any legal or reputational risks involved in sharing personal information can be reduced to an acceptable level (we may do this through carrying out a Data Protection Impact Assessment).
		- We will only share information if the legal or reputational risks can be reduced to an acceptable level.
		- We will record that we have considered potential conflicts of interest on our Record of Sharing.
	+ Where an organisation that is not a public authority wishes to sign this Agreement in order to share personal information pursuant to Part 5 of the Digital Economy Act 2017, then a sponsoring public authority will be required to have carried out an assessment of that organisation’s systems and procedures. This must be supported by a privacy impact assessment that is compliant with the Information Sharing Code of Practice: Public Service Delivery, Debt and Fraud.
* We recognise that organisations or public bodies who are signatories to this Agreement may decide to withdraw from the Agreement. To do so, they must give three months written notice to the K-MIP Chairman [see the [K-MIP portal](https://fs.klz.org.uk/adfs/ls?version=1.0&action=signin&realm=urn%3AAppProxy%3Acom&appRealm=3c3b1b19-418e-e711-941b-001018f502cb&returnUrl=https%3A%2F%2Fportals.kentconnects.gov.uk%2F&client-request-id=78611EBB-CE54-0000-D49D-707854CED301) for contact details].
1. **Reviewing and administering this Agreement**
* K-MIP will have a Chairman, chosen annually by the members of K-MIP.
* K-MIP will hold quarterly meetings, which will be called and convened by the K-MIP Chairman.
* We will review this Agreement annually at a K-MIP meeting.
* We will each ensure that our staff members receive thorough training about this Agreement and how to share personal information in compliance with its requirements. As a minimum, the training will address:
* the benefits of data sharing;
* how much should be shared;
* the challenges of data sharing in terms of maintaining public trust and respecting personal privacy;
* what powers exist to share data;
* the conditions under which data may be shared;
* what restrictions exist and which exemptions may apply;
* what other arrangements need to be in place before data is shared.
* If we require legal advice relating to this Agreement or on data protection, we will obtain that advice from our own legal advisors and not from the K-MIP Chairman.
* **Complaints from the public:** We will use our standard procedures to deal with complaints from the public arising from information sharing under this Agreement.
	+ If a complaint raises an issue which has implications for the drafting of this Agreement, it should be notified to and dealt with in consultation with the K-MIP Chairman.
* **Concerns over or complaints about the operation of this Agreement:**
	+ If we are uncertain as to what personal information can or cannot be shared under this Agreement, then we should escalate a query to our DPO or a senior staff member.
	+ If we have a complaint about the way in which information has been shared under this Agreement, then we should in the first instance, seek to resolve the complaint between ourselves. If that does not resolve the complaint, it should be escalated to the K-MIP Chairman for further action.

22 May 2018

**SIGNATORY ORGANISATIONS TO THE KENT AND MEDWAY INFORMATION SHARING AGREEMENT**

**We the undersigned agree that each organisation that we represent will adopt and adhere to this Agreement:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Organisation** | **Name and Signature of Head of Organisation** | **Name and Signature of DPO/IG Officer/SIRO** | **Date of Joining** | **Conflicts Declared?** |
|  |  |  |  | **Yes** [ ] No [ ] N/A [ ]  |
|  |  |  |  | **Yes** [ ] No [ ] N/A [ ]  |
|  |  |  |  | **Yes** [ ] No [ ] N/A [ ]  |
|  |  |  |  | **Yes** [ ] No [ ] N/A [ ]  |
|  |  |  |  | **Yes** [ ] No [ ] N/A [ ]  |

**DECLARATION OF CONFLICTS OF INTEREST**

We recognise that it is an important aspect of transparency and managing risks that we declare any potential conflicts of interest that might have an impact on our sharing of personal information. Such conflicts may arise from other work we do for public authorities or from our own commercial interests e.g. a competing loyalty between an organisation we owe a primary duty to and some other person or entity.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation** | **Declaration of Conflicts of Interest** | **Name and Signature of Head of Organisation** | **Name and Signature of DPO/IG Officer/SIRO** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Data Protection

Impact Assessment

You should start to fill out the DPIA at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| **Multi- Agency Safeguarding Hub (MASH)**For many years, the sharing of appropriate information about children who may be at risk with local authority social services has been vital in ensuring that as far as is possible the welfare of children is safeguarded. Research and experience has demonstrated the importance of information sharing across professional boundaries. The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant partner agencies - which include the police, children’s services authorities, Clinical Commissioning Groups and the NHS Commissioning Board - must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act as relating to a child’s: 1. Physical and mental health and emotional well-being (‘be healthy’) 2. Protection from harm and neglect (‘stay safe’) 3. Education, training and recreation (‘enjoy and achieve’) 4. The contribution made by them to society (‘make a positive contribution’) 5. Social and economic well-being (‘achieve economic well-being’) Although most commonly used to refer to young people aged 16 or under, ‘children’ in terms of the scope of this Act means those aged nineteen or under. Information upon which safeguarding decisions in relation to children and young people are made is held by numerous statutory and non-statutory agencies. Many tragic cases across the UK have highlighted deficiencies within safeguarding partnerships in relation to the sharing of information and communication. Serious case reviews and inquiries (such as Laming, Bichard) have directly attributed the lack of good information sharing and communication to the subsequent death of an individual. In order to deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information picture concerning an individual and their circumstances to be available to them. Information viewed alone or in silos is unlikely to give the full picture or identify the true risk. Therefore, all the relevant information from various agencies needs to be available and accessible in one place. A Multi-Agency Safeguarding Hub (MASH) helps ensure this and aids communication between all safeguarding partners. By ensuring all statutory partners have the ability to share information, it will help to identify those who are subject to, or likely to be subject to, harm in a timely manner, which will keep individuals safe from harm and assist safeguarding partners in discharging their obligations under the Act. MASH helps deliver three key functions for the safeguarding partnership; **1. Information based risk assessment and decision making** Identify through the best information available to the partnership those children and young people who require support or a necessary and proportionate intervention. **2. Victim identification and harm reduction** Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions. **3. Co-ordination of all safeguarding partners** Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and co-ordination of harm reduction strategies and interventions. The MASH model is highlighted as an example of good practice in multi-agency partnership working because of how it improves information sharing between participating agencies. The information sharing via Medway MASH is supported through the Kent & Medway Information Sharing Agreement and the accompanying Record of Sharing document. The Information Commissioner’s Office (ICO) requires completion of a DPIA when processing is ‘likely to result in high risk’. It is recognised that the processing conducted via MASH is* processing that is likely to result in a high risk to the individuals.
* processing of such a nature that a personal data breach could jeopardise the health or safety of individuals.
 |

Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| How will you collect, use, store and delete data? |
| * Data is collected via MASH partners and referrals via SPA.
* Data is stored on the child’s electronic record Framework I. Records are only accessed by authorized personnel.
* Records are retained/deleted in accordance with local authority record’s retention policy.
* Please refer to Appendix 1 for data flow.
 |
| What is the source of the data? |
| Safeguarding Referral are received by Single Point of Access (SPA) in Medway Children’s Services. The referrals could be received from any partner organization or members of the public. |
| Will you be sharing data with anyone? |
| Data will be shared with MASH partners.MASH is a consent based model and therefore information is only shared with informed consent unless to do so would further impact on the well-being of the child (GDPR article 6(1) (d) Vital Interests) or the prevention or detection of a crime. |
| What types of processing identified as likely high risk are involved? |
| The Information Commissioner’s Office (ICO) has identified this type of processing as ‘likely to result in high risk’. It is recognised that the processing conducted via MASH is* processing that is likely to result in a high risk to the individuals.
* processing of such a nature that a personal data breach could jeopardise the health or safety of individuals.
 |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| * Data is personally identifiable information contained in Medway Council Social Care Records and/or data from partner organisations.
* Information may be opinions given by referees and/or partner organisations.
* It is likely the data will be special category data and may be criminal offence data where relevant to the case.
* The quantity and frequency of data sharing is proportionate and relevant to the case and only shared when necessary and when the relevant exemptions apply.
* Records are retained/deleted in accordance with local authority record’s retention policy.
* It is not possible to quantify the number of individuals affect, it could vary at any given time.
* The data is specific to Medway Council service users, however, data could be shared/sourced worldwide if deemed appropriate to the case.
 |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| * Individuals will be service users of the services provide by all MASH partners.
* MASH is a consent based model and therefore information is only shared with informed consent unless to do so would further impact on the well-being of the child (GDPR article 6(1) (d) Vital Interests) or the prevention or detection of a crime.
* The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant partner agencies - which include the police, children’s services authorities, Clinical Commissioning Groups and the NHS Commissioning Board - must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Therefore, there is an expectation that MASH partners would use personal data in this way.
* The data is highly likely to include children and vulnerable groups.
* The council has security protocols in place to ensure safe electronic transfer of data. However, there will always be the element of risk as a result of human error, the council provides regular data protection training to mitigate this risk.
* All social workers are bound by the HCPC code of conduct.
 |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?  |
| To deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information picture concerning an individual and their circumstances to be available to them. Information viewed alone or in silos is unlikely to give the full picture or identify the true risk. Therefore, all the relevant information from various agencies needs to be available and accessible in one place. A Multi-Agency Safeguarding Hub (MASH) helps ensure this and aids communication between all safeguarding partners. |
| MASH helps deliver three key functions for the safeguarding partnership; **1. Information based risk assessment and decision making** Identify through the best information available to the partnership those children and young people who require support or a necessary and proportionate intervention. **2. Victim identification and harm reduction** Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions. **3. Co-ordination of all safeguarding partners** Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and co-ordination of harm reduction strategies and interventions.  |
| The MASH model is highlighted as an example of good practice in multi-agency partnership working because of how it improves information sharing between participating agencies. |

Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| Data Protection Officer has been consulted in the preparation of this document and is informed of the MASH process. |
| All MASH partners are consulted on a regular basis regards this process. |
| Governance sits with the Director of Children’s and Adults Services who is also the Caldicott Guardian for Medway Council. |
| All partners are held to account by Medway Safeguarding Children’s Board. |
| Information Security: Medway Council’s ICT Security team ensure the council is compliant with necessary cyber security protocols. |

Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| **The lawful basis for processing is:** GDPR Article 6:Processing shall be lawful only if and to the extent that at least one of the following applies:1. Consent[[3]](#footnote-3) [x]
2. Contract[[4]](#footnote-4) [ ]
3. Legal Obligation[[5]](#footnote-5) [ ]
4. Vital Interests[[6]](#footnote-6) [x]
5. Public Task[[7]](#footnote-7) [x]
6. Legitimate Interests[[8]](#footnote-8) [ ]

*(tick all relevant boxes)***In accordance with the following statutes:**Children Act 1989 and 2004Working Together 2018 |
| MASH data within Frameworki is securely stored and only access is given to authorized individuals, this prevents function creep.Anonymised data may be used to inform service development. |
| Regular multi-agency audits are undertaken to quality assure information held Frameworki |
| Individuals are referred to the Council’s privacy notice and advice on the council’s website about how to exercise their rights. |
| International data is usually verbally on the phone, data is unlikely to be shared electronically. However, if it was necessary relevant security protocols/encryption would be used. |

Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary.  | **Likelihood of harm** | **Severity of harm** | **Overall risk**  |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
| Data accessed by unauthorized personnel | Remote | Severe | low |
| The council has security protocols in place to ensure safe electronic transfer of data. However, there will always be the element of risk as a result of human error. | Possible | Severe | Medium |
| Risk of function creep and data being used for matters other that for which it was collected. | Remote | Severe | Low |

Step 6: Identify measures to reduce risk

|  |
| --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** |
| **Risk**  | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |
| Data accessed by unauthorized personnel | Three entry log in system | reduced | low | yes |
| The council has security protocols in place to ensure safe electronic transfer of data. However, there will always be the element of risk as a result of human error.  | The council provides regular data protection training to mitigate this risk and regular supervision of staff.The KMISA, to which all partners are signatories, requires that they ensure staff are trained. | reduced | low | Yes |
| Risk of function creep and data being used for matters other than for which it was collected. | MASH data within Frameworki is securely stored and only access is given to authorized individuals, this prevents function creep. | reduced | low | yes |

Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item**  | **Name/date** | **Notes** |
| Measures approved by: | Ian Smith20/12/18 | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Ann Domeney20/12/18 | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | Gayle Jones20/12/18 | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:I am content that this DPIA is satisfactory and processing may continue. However, further consultation is required with ICT and evidence of consultation with partners will need to be addressed early in 2019.This document will also need to go through the next Security and Information Governance Group, for information and comment only.  |
| DPO advice accepted or overruled by: | Ian Sutherland20/12/18 | If overruled, you must explain your reasons |
| Comments: |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |

**Appendix 5:**

**List of MASH Professional Lead contacts**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Agency:** | **Lead Contact** | **Tel/Secure Email:** | **Alternative contact** | **Tel/Secure Email:** |
| Children’s Social Care | Kelly Cogger | Kelly.cogger@medway.gov.uk | Ian Smith | Ian.smith1@medway.gov.uk |
| Police | Heather Thompson | heather.thompson@kent.pnn.police.uk | Sam Mercer | Samantha.mercer@kent.pnn.police.uk |
| Health Partners | Ida Bradford | i.bradford@nhs.net | Penny Giles McLoughlin | p.giles@nhs.net |
| Education  | Stephanie Ponter | Stephanie.ponter@medway.gov.uk | Christine Impey | Christine.impey@medway.gov.uk |
| Youth Offending Services | Davina Munn | Davina.munn@medway.gov.uk | Ken Dance | Ken.dance@medway.gov.uk |
| Housing  | Ray Easdown | Ray.easdown@medway.gov.uk | Mark Breathwick | Mark.breathwick@medway.gov.uk |
| Early Help Service | Lorraine Redmond | Lorraine.redmond@medway.gov.uk | Andrew Willets | Andrew.willetts@medway.gov.uk |
| 0-25 SEND | Alison Mills Clarke | Alison.millsclarke@medway.gov.uk | Wendy Vincent | Wendy.vincent@medway.gov.uk |
| NPS: Probation Service | Clare Hastings | Claire.hastings@justice.gov.uk | Tine Hughes | Tina.Hughes1@justice.gov.ukPh: 01622 617402 |
| NPS: CRC | David Gardner | David.gardner@ksscrc.co.uk | Emma Vecchiolla | Emma.vecchiolla@ksscrc.co.uk |
| Open Road | Amy Mckeown | amy.mckeown@turning-point.co.uk |  |  |

1. Information Sharing: Guidance for practitioners and managers. DCSF p21. [↑](#footnote-ref-1)
2. As above p22 [↑](#footnote-ref-2)
3. [Consent | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) [↑](#footnote-ref-3)
4. [Contract | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/) [↑](#footnote-ref-4)
5. [Legal obligation | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/) [↑](#footnote-ref-5)
6. [Vital interests | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/) [↑](#footnote-ref-6)
7. [Public task | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/) [↑](#footnote-ref-7)
8. [Legitimate interests | ICO](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/) [↑](#footnote-ref-8)