Kent & Medway Information Sharing Agreement 2013-14

CONTENTS

Introduction

Parties to this Agreement

The organisations that have undertaken to adhere to this Agreement are detailed on the Kent Connects Portal:

http://www.kentconnects.gov.uk/portals/infosharing/kent-medway-information-sharing-agreement/signed-copies-of-information-sharing-agreement-from-partners

Each organisation formally undertakes to ensure protocols and procedures to share information accord with this Agreement:

The current version of the Agreement is available via the Kent Trustweb:

https://www.**kenttrustweb**.org.uk/Policy/dpfoi_info**sharing**.cfm

Information Exchanges with Non Signatory Organisations

If information is to be disclosed to a non-signatory organisation, it is the responsibility of the disclosing organisation to satisfy itself that legitimate and justifiable grounds exist, and that the necessary confidentiality and security standards and safeguards are in place before the information is disclosed.

The organisations may be legally obliged to register processing of data with the Information Commissioner. It follows that organisations consequently have a duty to train their personnel to appreciate the legal requirements of the Data Protection Act and the Common Law Duty of Confidence and, in particular, their individual culpability.

Signatory organisations are expected to encourage non-signatory organisations providing services in either Kent or Medway to also become signatories.

Private and Voluntary Organisations

The involvement of private and voluntary organisations in the provision of public services is increasing. Where such services are to be provided by private or voluntary organisations, those organisations should also be signatories to this Agreement.

In exceptional circumstances, information may be disclosed to non-signatory organisations if assurances have been given that the appropriate safeguards are in place, but the responsibility will rest with the disclosing organisation.

Purpose of this Agreement

The purpose of this Agreement is to:

- provide a framework for embedding best practice with regard to the disclosure and exchange of information between those organisations responsible for the delivery of public services in Kent and Medway;
- acknowledge the need for partner organisations to share information proactively, i.e. without a request first having to be made, where one partner identifies a need to share with another;
- set out the legal gateway through which the information is shared, including reference to the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidence (this Agreement does not overrule either Acts, the Common Law Duty of Confidence, or the right not to disclose privileged information, such as the communication between a legal adviser and their client);

- describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities, including under the Data Protection Act 1998 and any partner specific security requirements;
- provide a generic standard to be applied for the various specific purposes, for which the signatory organisations have agreed to share information. This may be specified in a separate Standard Operating Procedure (SOP) provided for each purpose (see **Appendix B** for the standard template and **Appendix C** for live procedures);
- clarify the understanding between signatories to this Agreement of each party's responsibilities and duties towards the other;
- describe the roles and structures that support the exchange of information between partner organisations;
- ensure compliance with individual partners' policies, legal duties and obligations.

Review of the Agreement

The Information Governance Programme Board is responsible for conducting annual reviews of this Agreement in February of each year and for reporting to the Joint Kent Chief Executives on the main findings and for proposing any changes during the first quarter of each new financial year.

The annual reviews will:

- consider whether the Agreement is fit for purpose, including, where relevant, the specific sets of Standard Operating Procedures held on the IGPB Portal;
- identify any emerging issues, such as new legislation, national guidance or local experience;
- determine (offer advice) whether the Agreement should be extended for a further period (up to one year) or whether to terminate it.

Standard Operating Procedure

This Agreement provides a Standard Operating Procedure template (**Appendix B**) which signatories will use to support specific information exchanges.

The Standard Operating Procedure enables organisations planning to disclose information to set out their decisions as to:

- the types of information which will be disclosed.
- the method to be used to disclose that information;
- the parties and their contact details;
- the purpose and type of event that may trigger the need to disclose;
- the administration/process to be adopted;

Each Standard Operating Procedure will have a review schedule with the current version indicating the date for the next review.

Legislation, Codes of Practice and Guidance

The relevant legislation, codes of practice and guidance are listed at **Appendix G**. These provide the gateways for signatory partners to share information and must be complied with.

Golden Rules

Each signatory organisation will ensure that their staff:

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to enable the appropriate sharing of personal information about living persons.

2. Are open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so. Consent should be reviewed on a frequent basis with those who have given it so that it is always current.

3. Seek advice if they are in any doubt, without disclosing the identity of the person where possible (e.g. by referring to a Primary Designated Officer or Designated Officer).

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Information may still be shared without consent if, in their judgement, that lack of consent can be overridden in the public interest. They will base their judgement on the facts of the case.

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

6. Apply the following principles when sharing information, "necessary, proportionate, relevant, accurate, timely and secure", ensuring that the information shared is necessary for the purpose for it is being shared, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep records of their decisions and the reasons for them – whether it is to share information or not. If the decision is to share the record will indicate what has been shared, with whom and for what purpose.

Each signatory organisation will:

1. promote the Rules amongst members of their staff who at any time may be responsible for the exchange of personal and sensitive data with another (signatory) organisation

2. Include the above rules in any Standard Operating Procedure agreed with partner organisations.

Sensitivity of Data and Information Sharing Practice

The definition of personal data is complex and for day to day purposes it is best to assume that all information about a living, identifiable individual is personal data.

Non-Personal Data

Information which does not relate to a living, identifiable individual is not personal data.

For example aggregated data, derived from personal, non-personal and depersonalised data that is used for management information purposes such as needs analysis, service planning, crime profiling and performance measurement.

Depersonalised Data

Depersonalised data encompass any information extracted from personal data that does not and cannot be used to establish the identity of a living individual.

It must be noted that, for example, even a post-code or address can give away the identity of an individual if there is only one person living there.

It is good practice for signatory partners, where possible, to give data subjects information about how depersonalised data about them may be used.

Privacy Notices can be used to provide this information.

Personal Data

Personal data is data, which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller (the organisation collecting and so owning the data).

This data must be clearly marked as personal data and kept securely within a password protected and encrypted computer system or otherwise physically secure with appropriate levels of staff access.

Portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Partners must undertake to destroy all personal information when no longer required for the purpose for which it was provided (please refer to the section on Security & Data Management, below).

Signatory organisations undertake to:

- formally record all grounds for disclosure of personal information;
- process information fairly and objectively for each case;
- only disclose sufficient information to enable partners to carry out the relevant purpose for which the data is intended, determined on a case-by-case basis.

Sensitive Personal Data (as defined by the Data Protection Act 1998)

Sensitive personal data is data that falls into the following categories:

- racial or ethnic origin;
- sexual life;
- physical or mental health;
- membership of a trade union;
- political or religious beliefs;
- criminal offences and proceedings.

Where signatory organisations process sensitive personal data, they need to satisfy both a condition of schedule 3 of the Data Protection Act 1998 as well as a condition of schedule 2.

Any disclosure of personal or sensitive personal data should be restricted to the minimum necessary to achieve the purpose.

Decision to Share Personal Data

Personal information and data should only be disclosed in a particular case when the disclosing organisation is satisfied that:

- it is legally empowered to do so;
- the conditions of schedule 2 of the Data Protection Act 1998 are satisfied;
- the proposed disclosure of personal information is done in accordance with the principles of the Data Protection Act 1998 (DPA);
- the proposed disclosure of personal information observes the Common Law Duty of Confidence (below) and the principles of the Human Rights Act 1998 (HRA).

Common Law Duty of Confidence

Obtaining **the valid consent of a data subject** enables the disclosure and use of relevant information for the purposes for which that consent was given and should be obtained when ever possible.

The key principle is that information confided should not be used or disclosed further, except as originally understood by the data subject, or with their subsequent permission.

To give proper consent to disclosure, the data subject must be informed of the nature of the information to be revealed, to whom it will be revealed, the purpose for which the information will be used and the potential consequences.

Data subjects (e.g. patients, service users) can consent only to limited disclosure for a limited purpose (such as disclosure limited only to physical health issues and excluding mental health issues) and any limits on the consent must be respected. Care should be taken not to involuntarily identify other individuals whose consent has not been sought or obtained.

If consent is not given, then signatory organisations need to decide on a case-by-case basis whether to disclose any information that they may have on an individual. In these circumstances, a decision may be required as to whether an individual's private right to confidentiality is outweighed by a public interest in, for example, a need to protect either the public or the health and safety of the individual.

Where the decision to disclose is made, again depending upon individual circumstances, it is usually appropriate to notify the data subject that the disclosure is going to be made.

As the duty of confidentiality is not absolute, there might be circumstances where the public interest in maintaining confidentiality is outweighed by the public interest in disclosing specific information. Such circumstances may include where disclosure is necessary to avert a real risk of a danger of death or serious harm to others or for the prevention or detection of serious crime. Even then, such disclosure is permissible only if made to someone with a proper interest in receiving the information.

The pubic interest test consists of one or more exceptional circumstances (see below) that justify overruling the right of an individual to confidentiality in order to serve a broader pubic interest.

Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of the public in the continued provision of for example a confidential service. The public interest test threshold for disclosure where an individual has withheld their consent is generally stronger than where it has not been possible to seek their consent.

Confidentiality can also be overridden or set aside by legislation.

Caldicott Guardians and Guidelines on Information Sharing

HSC 1999/012, HSC 2002/003 and LAC (2002)2 require all NHS and Social Care organisations to appoint a Caldicott Guardian who will act as the 'gatekeeper' of information relating to both individuals and population groups. .

NHS & Social Care organisations must have procedures to control access to patient/person identifiable information. The Caldicott Guardian should agree who has access to what information.

Caldicott Guardians can delegate their information sharing responsibilities, if they so wish, to someone else in their organisation. This person must be familiar with current legislation, guidance and best practice and must have a route for escalating any concerns they may have before making a decision as to whether information should be shared.

The Caldicott Guidelines affirm the individual's wishes should be respected unless there are exceptional circumstances. However they are not law. The Data Protection Act, the Human Rights Act and Common Law will always take precedence.

Similarly, in relation to the Department of Health document "No Secrets" (2000) approach, it is inappropriate for agencies to give assurance of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when persons may be at risk.

Legislation v Common Law

If there is an apparent conflict between legislation and common law, the legislation will take precedence.

Exceptional circumstances may arise, for example, where there is a serious public health risk, or there is a risk of harm to a patient or other individuals, or for the prevention, detection or prosecution of crime.

There are occasions, therefore, where seeking the individual's consent is not always appropriate. Information held in confidence can still be disclosed without the individual's consent, where it can be demonstrated that:

- disclosure is required by law (e.g. under an Act of Parliament creating a statutory duty to disclose or a court order);
- disclosure is necessary for the detection, prevention and prosecution of crime or the apprehension of offenders;
- information is already clearly in the public domain;
- there is an overriding duty to the public that outweighs maintaining public trust in a confidential service and the duty of confidence to the individual (e.g. health and safety);
- there is a risk of death or serious harm to one or more other individuals or the public at large;
- the individual lacks the capacity to make an informed decision for themselves (e.g. where a patient is incapable of giving consent then any disclosure which is in their best interests would be permissible);
- in the vital interest of the individual concerned (e.g. information relating to a medical condition may be disclosed in a life or death situation).

Public Interest

Public interest criteria will include, but is not limited to:

- health and safety;
- prevention and reduction of crime and disorder;

- detection of crime;
- apprehending offenders;
- protection of persons at risk within the community;
- administration of justice;
- national security.

Signatory organisations need to clearly establish, in each case, these considerations are sufficient to override the Common Law Duty of Confidence and that the disclosure is strictly necessary for these purposes.

Proportionality of the data sharing

The Human Rights Act 1998 incorporating the European Convention on Human Rights restricts public authorities in its use of private information.

Article 8, the Right to Respect for Private and Family Life is the most commonly referred to article when considering and dealing with requests for disclosure of information.

The right is qualified, in that it may be interfered with where this is in accordance with the law and is necessary in a democratic society:

- in the interests of national security;
- in the interests of public safety;
- in the interests of the economic well being of the country;
- for the prevention of disorder or crime;
- for the protection of health or morals; or
- for the protection of the rights and freedoms of others.

When the human rights of any individual are considered to be actually or potentially engaged by a disclosure under the Agreement, the Primary Designated Officer(s) and Designated Officer(s) (see below) involved should ask themselves whether there is a statutory basis for the processing and whether their actions are **(JAPAN)**.

- **J**ustifiable
- **A**ppropriate
- **P**roportionate
- **A**uditable
- **N**ecessary

To be proportionate the disclosure must only go as far as is necessary to achieve the desired aim.

Necessity of the data sharing

All decisions to disclose data must be made on a case-by-case basis and in every instance the level of that disclosure may be different.

Only the Primary Designated Officer or nominated Designated Officers of an organisation can agree to disclose to another organisation.

To determine whether data should be disclosed the Primary Designated Officer or Designated Officer must compare the specified legal authority against the following (but not exclusive) issues:

- relevance of the request to the aim

- proportionality
- data quality
- method of disclosure
- conditions of disclosure
- details of the decision making process

Fair Processing of the Data

The Data Protection Act 1998 requires the fair processing of personal data unless an exemption applies.

Fair processing means:

- the individual knows what is happening to their personal data;
- the use of the data is, in the general sense of the word, fair to that person.

The Portal includes examples of Fair Process Notices that may be used by signatory organisations as does the website for the Information Commissioner's Office.

The most likely exemptions to being fair are where data is necessarily shared for:

- the prevention and detection of crime or the apprehension or prosecution of an offender;
- the purpose of protecting the welfare of a child or a vulnerable adult when they are assessed as being at risk from another person.

The Information Sharing Process

Roles and responsibilities

Primary Designated Officer (PDO)

Each signatory organisation appoints a Primary Designated Officer for each sharing purpose within the part of the business in which it functions. The Primary Designated Officer will:

- be a manager of sufficient standing to have a co-ordinating and authorising role;
- be the Specific Point of Contact (SPOC) for their organisation for the specific sharing purpose.
- maintain an overview of all requests that have been issued or received within their remit and keep an updated list of Designated Officers for their body
- ensure all requests for information under this Agreement and responses are recorded and auditable
- ensure a deputy is identified in their absence
- ensure records of security arrangements made to protect the integrity and confidentiality of the request and disclosure files are maintained
- on a case-by-case basis will ensure personal data is processed lawfully and **be responsible for the final decision on whether to share information (see also "Sharing Concerns Between Partners", below)**;
- appoint one or more Designated Officer(s) to act on their behalf when necessary as daily users of this Agreement ensure that all Designated Officers are fully trained and aware of their responsibilities

Designated Officer (DO)

- may manage the majority of the work (at the discretion of the PDO) and refer to the PDO for action or guidance where appropriate.

A central register of the identities and contact details of PDOs and DOs must be maintained by each signatory organisation. These details must be notified to all other signatory organisations via the Portal within 28 days of such change occurring.

Voluntary Organisations, Agencies, Representatives and Sub-Contractors

Voluntary organisations, agencies, representatives and sub-contractors (including any employees of sub-contractors) employed/contracted by signatory organisations, must abide by the same constitution, codes of practice, operating guidelines and data protection agreements as the partners.

This requirement must be included in any formal contract between a signatory organisation and any provider of a service they have commissioned.

The Selected Method(s) for Information Sharing

The selected method(s) will vary depending upon the circumstances in which information is disclosed. For example, there may be a shared office environment, partners may work from their remote sites or there could be a combination of both.

Appendix C provides details of the requirements for each alternative.

Security & Data Management

General

Signatories to this agreement must:

- have clear policies with respect to the secure management of data, including on personal devices where they are used by staff;
- adhere to the standards adopted by the information source Data Controller to meet the terms of the Data Protection Act 1998 and in particular the seventh principle in Part 1 of Schedule I of that Act and ISO27001 (Information Security Management).

Individual signatory organisations are responsible for ensuring that they have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information held.

All information shared under this Agreement must be protectively marked in accordance with Cabinet Office advice contained in Security Vetting and Protective Markings: A Guide for Emergency Responders (March 2008). A copy is in ***Appendix A****.*

NB the new guidance will be included once it is published which is now expected to be April 2014.

Personal information must <u>not</u> be discussed, faxed, text (SMS) sent, or emailed over public/mobile telephone or unsecured email links, except in cases of urgency (e.g. potential danger to life - see also Appendix C "Information Sharing Method 5 Operationally Urgent"). Only the minimum amount of information necessary to achieve the purpose should be disclosed.

Partners must adhere to parts 3.16 to 3.19 of the Cabinet Office Security Vetting and Protective Markings Guide, referred to above, for full compliance.

Data Storage, Retention, Review and Disposal

Signatory organisations must have a clear policy relating to data storage and retention, which identifies the posts that are accountable for the actions set out in the remainder of this section.

The information disclosed must be stored securely and destroyed, or returned to the original disclosing organisation, when it is no longer required for the purpose for which it was provided.

Each live project file must be reviewed annually from the date of its creation for this purpose. Destruction must be by way of shredding; using crosscut shredding machines and/or electronic shredding software as a minimum.

Data Accuracy and Updating

If other information available to the requesting organisation, at the time or later, suggests that the information provided is inaccurate or incomplete, they should at the earliest possible moment inform the supplying Designated Officer concerned of such inaccuracy or incompleteness.

Risk Management

Signatory organisations recognise that the disclosure of information may expose that information to risk of accidental or deliberate misuse or inappropriate disclosure. Signatory organisations are committed to reducing such risks and acknowledge that any deliberate use or further disclosure of personal data shared under this Agreement in a manner inconsistent with this Agreement is likely to be regarded as a criminal offence under Section 55 Data Protection Act1998.

Sharing Concerns between Partners

Any concerns regarding information exchanged under this Agreement should be communicated to the relevant signatory organisation's staff responsible for handling/investigating data protection and/or information security complaints and the Senior Information Risk Owner (SIRO) or equivalent.

All data disclosed is subject to the recognition that both the original owner and the recipient have the responsibility of "Data Controller" with respect to its management. Each organisation is responsible for ensuring that all data protection requirements are being effectively satisfied.

Where a Standard Operating Procedure is in place it should document how these responsibilities will be met.

Audit

Records management processes and procedures must support signatory organisations' audit requirements. All record keeping systems must be able to display a clear audit trail.

Complaints and Breaches

Complaints

Complaints must immediately be referred to the appropriate PDO for the relevant signatory organisation and that organisation shall apply its own adopted procedure for dealing with complaints.

Breaches

Any breach of confidentiality or security identified must immediately be referred to:

- the PDO of the organisation responsible for the breach
- the data subject by the organisation owning the data
- the Information Commissioner's Office

The signatory organisation responsible for the breach must apply its own adopted procedure for dealing with such events in order to prevent re-occurrence of the breach.

Freedom of Information

Freedom of information requests for access to information exchanged via this Agreement will be referred to the receiving organisation's Freedom of Information specialist(s).

Data Subject Access Request

Signatories to this Agreement will comply with subject access requests in accordance with the relevant legislation.

Where the relevant information has been provided by a third party or other signatory organisation, that party or organisation will be notified as soon as possible of the request and in any event before a response is given.

Indemnity

In consideration of the provision of information in accordance with this Agreement, each of the signatory organisations to this Agreement undertake to indemnify the other against legal liability for a negligent act or accidental error or accidental omission which may be incurred in circumstances where the subject of the exchange of information suffers loss as a result of the misuse or inaccuracy of the information and brings an action claim or demand as a consequence thereof.

Provided that this indemnity shall not apply:

- Where the liability arises from information supplied which is shown to have been incomplete or incorrect, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part;
- Unless the party claiming the benefit of the indemnity has notified the party against whom it intends to invoke the indemnity within 56 days of any third party action claim or demand and thereafter the parties shall consult as to how the party against whom the claim has been made should proceed in respect of such claim;
- If the party seeking to invoke the indemnity has made any admission, which may be prejudicial to the defence of the action, claim or demand.

Withdrawal from the Agreement by a Signatory Partner

Any signatory organisation may withdraw from this Agreement upon giving **three months written notice** to the other signatories.

Data, which is no longer relevant, should be destroyed or returned.

Signatory organisations must continue to comply with the terms of this Agreement in respect of any data that the partner has obtained through being a signatory.

Signatories

Each organisation will sign a Signatory Form (**Appendix D**) to confirm compliance with relevant legislation, acceptance of the terms of this Agreement, responsibility for its execution and a commitment to train staff in order that requests for information and the process of sharing itself is sufficient to meet the purposes of this Agreement.

Signatories must also confirm their acceptance of the terms of the Standard Operating Procedure(s) relevant to their organisation (**Appendix B**) and listed on the Signatory Form. A

revised Form will be signed by each organisation when all parties involved agree changes to the Agreement or any Standard Operating Procedure relevant to that organisation.

The Information Governance Programme Board will hold original Signatory Forms with the Agreement and will co-ordinate proposed changes to this Agreement for submission to the Joint Kent Chief Executives for approval.

APPENDIX A - Security Vetting and Protective Markings

(The new guidance once published by the Cabinet Office will be included with the Agreement rather than being a separate document – publication is not expected before April 2014)

APPENDIX B - Standard Operating Procedure Template

This Template provides advice (in red) and the standard format and words (in black) to assist staff preparing a Standard Operating Procedure (SOP) document. (See live examples in Appendix C).

Title to be inserted

Information Sharing Agreement
Standard Operating Procedure.

Type of Agreement

This SOP is to be read in conjunction with the Kent & Medway Information Sharing Agreement and **Method XX (**Description to be inserted**)**. There is the option to include more than one Method.

Personnel involved in the information sharing process must be fully aware of the requirements of Agreement Method XX.

Parties to this Agreement and contact number to identify Primary Designated Officer (PDO)

List the parties to the specific agreement and contact numbers as indicated above. The details are to include the job roles as well of the names of the individuals currently holding those positions.

A list of regular PDO and Designated Officer (DO) contacts is to be maintained for easy reference and is to be attached to this document (electronic and paper version). If there is any doubt about the contact or the information requested check with your supervisor before disclosing information.

Purpose

List the purpose and the reason for considering the disclosure of information e.g. targeting/investigating crime and disorder incidents, notices seeking possession or eviction, child curfew notices or noise abatement investigations and notices.

Administration/Process

List specific administration/processes that are relevant to the particular SOP, such as the response times. There is always a need to specify how each partner will keep a record of decisions and the reasons, whether it is to share or not (see Golden Rules item 5, above). Apart from this requirement, there may not be a need to add more text if the standard wording provided in the Information Sharing Agreement (ISA) is sufficient. For example, the requirement for PDOs, a standard information sharing form and the need to keep records are all specified in the ISA, but if there is a need to identify other roles, vetting levels if required, or be specific about the format of a meeting/minutes additional information will need to be inserted here.

Information Disclosure Types (Examples)

Disclosure for the following relevant areas for each partner will be considered. Specific exclusions are also listed.

List information for which disclosure will be considered for each partner. Specific exclusions are also to be listed, if required (e.g. evidence in council led court cases will not be disclosed until the conclusion of the hearing)**.**

Signatory partners recognise that any data shared must be justified on the merits of each case.

Golden Rules

Each signatory partner will ensure their staff:

1. remember that the Data Protection Act is not a barrier to sharing information but provides them with a framework to ensure that personal information about living persons is shared appropriately.
2. are open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so. Consent should be reviewed on a frequent basis with those who have given it so that it is always current.
3. seek advice if they are in any doubt, without disclosing the identity of the person where possible (e.g. referring to a Primary Designated Officer or Designated Officer).
4. share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Information may still be shared without consent if, in their judgement, that lack of consent can be overridden in the public interest. They will base their judgement on the facts of the case.
5. consider safety and well-being, basing their information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. apply the following principles when sharing information, "necessary, proportionate, relevant, accurate, timely and secure", ensuring that the information shared is necessary for the purpose for it is being shared, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. keep records of their decisions and the reasons for them – whether it is to share information or not. If the decision is to share the record will indicate what has been shared, with whom and for what purpose.

Date of Next Review

The review of the Procedure will be completed by all partners to the Standard Operating Procedure by: _____

APPENDIX C – Alternative Sharing Methods

Information Sharing Method 1 - Form based, Non-urgent. (See Method 5 for classification and risk assessment to identify an urgent request)

This "Method 1" outlines the standards and processes to be applied when personal information is shared by partners in non-urgent circumstances and **using the application form attached to this Method 1** for a purpose identified by a Standard Operating Procedure (SOP) document (Appendix C).

A project file will be created to cover all aspects and documentation of the initiative/purpose and specify the objective it seeks to effect (for example an anti-social behaviour order against X in accordance with Section 1 (1)-(3) Crime & Disorder Act 1998). This will provide the audit trail.

This file will be managed by a named Primary Designated Officer (PDO) or Designated Officer (DO), who will ensure it is accurate and up to date. The relevant PDO will ensure information held is reviewed with partners by arrangement quarterly.

Where information is sought from partner bodies to support the aim of the initiative **an application will be made using the attached pro-forma**. Requests and responses should be made by PDOs or DOs of each Party to this Agreement.

Information to be provided in the request must include:

- The specific aim of the project, including the objective it seeks to effect;
- The nature of the information it seeks; and, if the information comprises personal data;
- The grounds for breaching any duty of confidence;
- Why the disclosure is in accordance with statutory provision, why the information is proportionate, necessary and relevant to achieving the aim;
- How fair processing will be achieved or why there is legal justification for the data subject not to be informed of the data-sharing;

The receiving PDO or DO will review the request and make a decision based on its arguments whether to disclose the information sought. The decision will be documented and the person seeking the disclosure informed of the result.

Disclosure of personal data to voluntary officers, agents, representatives and sub-contractors (including any employees of sub-contractors) employed/contracted by partners, must only be as provided for under the Data Protection Act 1998. The decision to disclose will necessarily have to be on a case-by-case basis and should not be regarded as being available under an automatic authority.

Response times will be specified in the SOP. The PDO or DO responding to the request will ensure copies of the correspondence are kept in accordance with the PDO's responsibilities under this Agreement.

The final decision in cases of difference of opinion lies with the PDO from whom information is sought. The PDO may wish to consult their internal specialist advisers in such cases.

RESTRICTED when complete (amend if required)

Request for Personal Information – Part 1

To:

Organisation:	
Name & Job Title/Rank:	
Contact address/details:	

From:

Organisation:	
Name & Job Title/Rank:	
Contact address/details:	
Reference:	

I am a Designated/Primary Designated Officer. In accordance with the justification specified in full below, I request personal information or sensitive personal information about:

Surname:	
All previous surnames:	
Also known as:	
Forenames:	
Place of birth:	
Date of birth:	
Full present address:	
Post code:	
Full previous address:	
Post code:	
Known identifier(s) e.g. Pupil ID, NHS number:	

Only the minimum amount of information to meet the requirement of the request should be disclosed and it will only be used for the purpose specified. The recipient will not release the information to any third party without obtaining the express written authority of the supplying organisation.

RESTRICTED when complete (amend if required)

RESTRICTED when complete (amend if required)

The subject of this request has given their consent, which is attached, or where this has not been obtained the specific statutory power, obligation or DPA exemption is set out below. The making of an unjustifiable request could constitute a criminal offence. Evidence must be provided to substantiate any disclosure being made where a public interest test is required and the public interest to disclose is considered to outweigh the interest to maintain a duty of confidence.

I confirm that the personal or sensitive information is required for the following purpose and with the following justification:

Please use continuation sheet, if required.

The information I require is:

Please use continuation sheet, if required.

Failure to disclose the information will have the following impact:

Please use continuation sheet, if required.

***I confirm that in accordance with S29 of the Data Protection Act the subject will not be informed of this disclosure, because to do so is likely to prejudice the prevention or detection of crime or the prosecution or apprehension of offenders.** * Delete if not applicable

Signed:		Date:	

RESTRICTED when complete (amend if required)

RESTRICTED when complete (amend if required)

Request for Personal Information – Part 2

Confirmation of Disclosure

To:

Organisation:	
Name & Job Title/Rank:	
Contact address/details:	
Reference:	

From:

Organisation:	
Name & Job Title/Rank/Force No.:	
Contact address/details:	
Reference:	

A list of the specific information to be disclosed is listed here (not the information itself which must be recorded separately).

Information to be disclosed:

Please use continuation sheet, if required.

I confirm that full consideration has been given and that I am satisfied the information listed above may be disclosed. This information is provided to you solely for the purpose set out within your request and must not be used for any other purpose without my prior and express written authority.

Signed:		Date:	

RESTRICTED when complete (amend if required)

Information Sharing Method 2 - Shared Environment

This "Method 2" outlines the standards and processes to be applied when partner agencies share personal information for a purpose identified by the relevant Standard Operating Procedure (SOP) document (See Appendix C) in a shared environment (e.g. multi-agency staff sitting in a shared office within one partner agency premises). This is distinct from the formal multi-agency meeting/conference environment (See Appendix D, Method 4). Where access to the host organisation's ICT is being provided this document will need to be read in conjunction with Appendix D, Method 3 – Direct Access to Partner IT System(s).

Where the environment is deemed to be a secure office, all partners' personnel details should be formally recorded in the format of the attached Schedule of Services & Personnel and attached to the SOP. If and when security vetting is required to gain access this will be specified in the relevant SOP (See Appendix C).

Details of the shared office (including details of the host organisation and location of the office) must be included in the Schedule of Services & Personnel.

Only the personnel included in the Schedule of Services & Personnel are authorised to access the office. Any visitors must be agreed with all associate partner agencies.

Where it is not possible to have a secure office made exclusively available to the partnership, the location will be regarded as a mobile working environment and partner's mobile working policy and procedures will apply.

Clear instructions must be developed for maintaining the physical security of the office (e.g. key management). All partners' personnel must familiarise themselves with these instructions and ensure that they comply.

Any changes to the environment or security arrangements, including the involvement of subcontractors, must be with the agreement of all partner agencies.

All personnel must familiarise themselves, and comply with, the Information Security Policy of all partner organisations party to the relevant SOP (See Appendix C).

All personnel must be fully aware of, and comply with, the requirements of the Government Protective Marking System/Scheme (See Appendix A). All protectively marked and sensitive documents must be stored and disposed of securely.

All copying, sharing and disclosure of information within the shared office must be strictly controlled and within the terms and conditions of this Information Sharing Agreement and the relevant SOP (See Appendix C).

All partner agencies must comply with the confidentiality and non-disclosure requirements contained in this Agreement, as well as all applicable laws, regulations and any contractual obligations of all parties.

All security incidents that could affect the security of information within the partnership must be reported and reviewed, both within the partnership and through each individual agency's normal reporting policy and procedure.

The security of all the partner agencies information and associated ICT must never be reduced by the introduction of this working arrangement.

Each partner acknowledges that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller as defined by the Data Protection Act 1998. The partner receiving the data will not use it for any purpose other than that specified in the original request, nor share it with any other party without the disclosing partner's written permission. The receiving partner remains a data controller in all other respects.

Primary Designated Officers are responsible for the final decision on whether to share information.

Schedule of Services & Personnel

Description of the facilities to be made available
Policies and Operating Procedures

List of Primary Designated Officers and Designated Officers (Users)

User Name	Reference	Access Requirement/Level	Date Added

Date updated: _____

Information Sharing Method 3 - Direct Access to Partner Information & Communication Technology (ICT)

This "Method 3" outlines the standards and processes to be applied where access to the host organisation's ICT is being provided. This will be for a purpose and in a designated physically secured environment (or by way of an approved mobile working solution) identified by the relevant Standard Operating Procedure (SOP) document (See Appendix C). This document may, therefore, need to be read in conjunction with Appendix D, Method 2 – Shared Environment.

All partner Primary Designated Officers (PDOs) or Designated Officers (DOs) details, as users of this Agreement, must be formally recorded in the format of the attached Schedule of Services & Personnel and attached to the SOP.

Only authorised PDOs/DOs identified in the Schedule of Services & Personnel are permitted access to the host organisation's ICT.

All PDOs/DOs must be vetted as specified in the relevant SOP (See Appendix C) to the appropriate level for the systems for which they are being granted access to.

Any changes to personnel, including leavers and joiners or vetting status, must be notified to the host organisation immediately.

All PDOs/DOs must be provided with a unique User ID, token and/or password for access to networks and systems.

All PDOs/DOs must be formally trained in the use of the systems for which they are being granted access to.

The organisation's ICT is provided for authorised business of the partnership only and within the terms and conditions of this Information Sharing Agreement and the relevant SOP (See Appendix C).

All PDOs/DOs must comply with applicable laws (such as the Data Protection Act), regulations and any contractual obligations of the host organisation.

All PDOs/DOs must comply with the host organisation's Information Security and ICT Acceptable Use Policies at all times.

All PDOs/DOs must comply with operating procedures defined for the systems in use.

PDOs/DOs must be fully aware of, and comply with, the requirements of the Government Protective Marking System/Scheme (See Appendix A).

No unauthorised modifications may be made to the host organisation's ICT and only that organisation will provide maintenance.

No attachments to networks or devices are permitted unless authorised by the host organisation.

All moves of non-portable ICT must be carried out by the host organisation.

The host organisation reserves the right to monitor and audit the use of all user activity on its networks and systems. The host organisation retains the right to withdraw access to its ICT services.

Any planned changes to a partner agency's physical security environment that has been surveyed or risk assessed for the protection of the host organisation's ICT, must be notified to the organisation in advance.

All copying, sharing and disclosure of information must be strictly controlled within the terms and conditions of this Information Sharing Agreement and the relevant SOP (See Appendix C).

All partner agencies must comply with the confidentiality and non-disclosure requirements contained in the associated agreements, as well as all applicable laws, regulations and any contractual obligations of all parties.

All security incidents or vulnerabilities that could affect the security of information or ICT services within the partnership must be reported and reviewed, both within the partnership and through each individual agency's normal reporting policy and procedure.

The security of all the partner agencies information and associated ICT must never be reduced by the introduction of this working arrangement.

Each partner acknowledges that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller as defined by the Data Protection Act 1998. The partner receiving the data will not use it for any purpose other than that specified in the original request, nor share it with any other party without the disclosing partner's written permission.

Primary Designated Officers are responsible for the final decision on whether to share information.

Schedule of Services & Personnel

Description of the facilities to be made available
Policies and Operating Procedures

List of Primary Designated Officers and Designated Officers (Users)

User Name	Reference	Access Requirement/Level	Date Added

Date updated: _____

Information Sharing Method 4 - Formal Meeting/Conference

Introduction

This "Method 4" outlines the standards and processes to be applied when partner agencies share personal information for a purpose identified by the relevant Standard Operating Procedure (SOP) document (See Appendix C) in a regular multi-agency meeting/conference environment.

Information sharing is strictly limited to the aims of the meeting/conference and, at the start of each meeting/conference, attendees will sign a confidentiality declaration in accordance with the example provided in the relevant SOP (See Appendix C). Information gained at the meeting/conference cannot be used for other purposes without reference and permission from the agency that originally supplied it, unless there are overriding concerns for safety of individuals, for example child protection concerns or safeguarding vulnerable adults (See also Appendix D Method 5 Operationally Urgent).

The relevant SOP (see Appendix C) will specify the detail to support the following general guidance:

Roles and Processes

Chair

The role of the Chair is to structure the meeting and prioritise referrals in such a way that all those attending are able to use the time available as efficiently as possible. The Chair will normally review incomplete actions agreed at the last meeting and make a record of any outstanding actions at the outset. Once actions are completed results should be fed back to the Coordinator in the form of timely updates.

It is the Chair's responsibility to ensure that all partner agencies understand precisely what is required of their agency either directly or indirectly. Those attending the meeting/conference must have a legitimate reason to be part of the process and should have the authority within their agencies to prioritise the actions that arise from the meeting/conference and be able to make an immediate commitment of resources to those actions.

At the start of each meeting the Chair will outline the confidential nature of the meeting and attendees will sign the confidentiality declaration mentioned in the Introduction above.

Coordinator

Each meeting/conference group will appoint a coordinator to administer and coordinate the process.

Identification

All partner agencies involved should have systems in place to recognise and identify individuals that need to be referred to the meeting/conference for discussion and the potential development of an action plan.

Referrals

All referrals should be made on a form(s) specified in the relevant SOP (See Appendix C). The coordinator will collect all information received for the meetings/conferences, identify and address any issues that arise, compile the agenda and send out a summary to partner agencies prior to the meeting/conference in sufficient time to ensure that all agencies have enough time to research their systems as specified in the relevant SOP (See Appendix C).

Agenda/Summary(ies)

The agenda structure should enable attendance for only part of the meeting/conference where a number of different referrals are reviewed, but are not relevant to all.

The agenda and summary(ies) will be sent to partner agencies via secure email and where this is not available information should be addressed to an individual by name or job title in a sealed envelope, marked 'Addressee only' and sent by post (or courier) with a return address showing. This is because all undelivered mail without a return address is opened at a Royal Mail sorting office, where staff are not security cleared (see Appendix A Security Vetting and Protective Markings for detailed instructions). Do **not** include the classification (e.g. "RESTRICTED") on the envelope.

The summary will include the reason for inclusion, name, DOB and addresses of parties involved but information will be kept as minimal as possible. The basic details are required to enable thorough searching of systems by partner agencies.

Once each agency receives the agenda they must research to see what information is held by their organisation. Dependent on the agency, when the agenda is received there may be actions to be completed prior to attending the meeting/conference.

Any late referrals may be discussed and decided with the relevant Coordinator and Chair as to whether they may be added.

The Meeting/Conference

Minute Taking

The Coordinator will take the minutes. The format of the minutes and the timescale for distribution are specified in the relevant SOP (See Appendix C). Distribution methods will adopt the same means outlined for the Agenda/Summaries, above.

Discussion

The Chair will invite the referring partner agency to present the details of their referral. The Chair will then invite partner agencies to present any proportionate and relevant information that their agency may have. It is expected that wherever possible partner agencies will always be represented (actions cannot be given to any partner agency not present). However, if this is not possible, it is expected that the representative from the partner agency who is unable to attend or send another designated officer, will forward any information to the Coordinator, which can then be shared at the meeting on behalf of the partner agency. This should ensure that all necessary information would be made available, even when certain agencies are not in attendance.

Disclosure

The meeting/conference has a general rule of confidentiality with the partner agencies involved as confirmed by the confidentiality declaration. The disclosure exclusion extends to staff employed by the agencies, but not involved in the process linked to the meeting/conference (need to know only). The only exception will be where the discussion and planning identifies the need to disclose to meet the aims of a plan adopted, it can be legally justified and is agreed by the partner agencies.

Action Planning

A tailored action plan, with timescales will be developed to meet the requirement, for example to increase the safety of a member of public or staff. Partner agencies are able to prioritise actions and provide support as required. There may be single actions but also combined actions between partner agencies. It is important that those relevant agencies are present as often as possible as actions can only be volunteered by persons present; the Chair is not able to task actions to any partner agency that is not present at the meeting.

Information Sharing Method 5 - Operationally Urgent

This "Method 5" provides guidance when the sharing of personal information is being considered in urgent circumstances for a purpose identified by a Standard Operating Procedure document (Appendix C).

It is recognised that there will be occasions when urgency is required (e.g. risk to life) when the need for disclosure and the method of disclosure must be weighed against the risk of a security breach, **for which the partner may be held accountable**. If it is decided that such transmissions are essential, they should be kept short and guarded speech used if, for example, a public/mobile telephone is used. Reference should be made to Cabinet Office advice contained in Security Vetting and Protecting Markings: *A Guide for Emergency Responders (March 2008)*. A copy is in Appendix A of this Kent and Medway Information Sharing Agreement.

Whether the decision is to disclose or not, an auditable record of the request and decision must be maintained. If disclosure is approved it is recognised that this may be a concession from normal data security requirements.

Each partner should deal with such matters in accordance with their organisation's established procedures. Sections of Kent Police Policies D14 and I13, to be found on the Force's web site (Kent Police Policy D14 Kent Police Policy I13), are examples. The policy will identify the level at which such decisions may be made and if in any doubt reference will need to be made to Legal and/or Data Protection experts within the organisation.

In summary the following points should be addressed and risk assessed against the decision-making factors before any disclosure takes place:

- **Who is asking for the information?**
- **Has the name, position, organisation and contact details of the enquirer been confirmed?**
- **What information is sought?**
- **Has a legal purpose to share information been established?**
- **Has appropriate authority for disclosure been sought and granted?**
- **Has the appropriate person, who may wish to seek advice from legal and or data protection advisors, authorised the disclosure?**
- **Record the decision, how it was made and what information was shared.**

APPENDIX D – Signatory Form

Kent & Medway Information Sharing Agreement (KMISA) New Partners Signatory Form

Completion of this Signatory Form confirms compliance with relevant legislation, acceptance of the terms of this Agreement, responsibility for its execution and a commitment to train staff in order that requests for information and the process of sharing itself is sufficient to meet the purposes of this Agreement. Signatories also confirm their acceptance of the terms of the Standard Operating Procedure(s) relevant to their organisation (Appendix C).

Organisation
Chief Executive (signature and print title/name)
Date
Information Sharing Lead, e.g. Data Protection Manager (print name and job title)
DPA Registration Number
ISO 27001 Registration Number (NB not mandatory for partners)

A revised Form will be signed by each organisation when all parties involved agree changes to the Agreement. The Information Governance Programme Board will hold original Signatory Forms with the Agreement and will co-ordinate proposed changes to this Agreement for submission to the Joint Kent Chief Executives for approval.

Appendix E Legislation

Legislation, Codes of Practice and Guidance

The following provide gateways and guidance for signatory partners to share information and must be complied with where relevant:

- Common Law (Duty of Confidence);
- Data Protection Act 1998 (Schedules 2 and 3);
- Human Rights Act 1998 (Article 8)
- Freedom of Information Act 2000
- Police Reform Act 2002 (Section 97)
- Adoption Act 1976
- Children Act 2004 Sections 10 & 11
- Education and Inspections Act 2006
- Criminal Justice Act 2003 (Section 325(4))
- Crime and Disorder Act 1998 (Section 115)
- NHS & Community Care Act 1990
- Health Act 1999 (Section 31)
- Professional Performance Act 1995
- NHS Act 2006 (Section 82)
- Health & Social Care Act 2001
- Medical Act 1983 & the Medical Act Amendment Order 2000
- Mental Health Acts 1983 & 2007
- Mental Capacity Act 2005
- Regulation of Investigatory Powers Act 2000
- Equality Act 2010 (particularly in respect of the public sector equality duty)
- Working Together to Safeguard Children (2010)
- Kent & Medway Safeguarding Children Procedures
- The Statutory Code of Practice for the Management of Police Information (2005)
- MAPPA Guidance 2009
- Information Sharing: Guidance for Practitioners & Managers (HMG 2008)
- Civil Contingencies Act 2004
- Learning and Skills Act 2000 (as amended)
- Data Protection and Sharing – Guidance for Emergency Planners and Responders
- Confidentiality: NHS Code of Practice (November 2010)
- Health and Social Care Act 2012