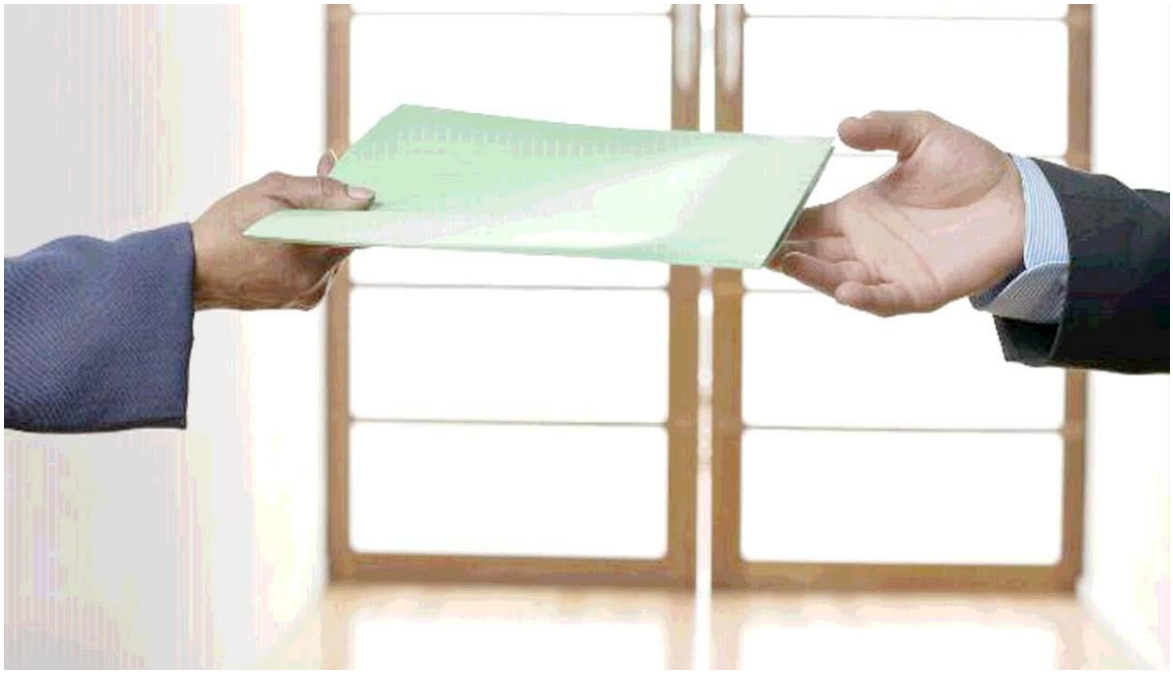
Surrey Multi-Agency Information Sharing Protocol (MAISP)



Last updated: 2014, Version 5.0

This protocol was developed by representatives on the Surrey MAISP User Group. All the organisations that sign up to the protocol are expected to take responsibility for ensuring they act in accordance with its principles.

Further information, including a list of organisations signed up to this protocol can be found on the Surrey County Council website:

http://www.surreycc.gov.uk/your-council/organisations-we-work-with/partnership-services-for-families/information-sharing-for-professionals/information-sharing-protocol-for-multi-agency-staff

CONTENTS

APPENDICES

SAMPLE FORMS

1. EXECUTIVE SUMMARY

Why we need an Information Sharing Protocol

1.1 Public bodies, private and voluntary organisations often have to collect personal information for a variety of reasons. These include:

- to plan and organise appropriate services for people
- to protect vulnerable people from harm
- to prevent crime
- to pool resources

1.2 Such information may vary from basic identification and contact details to more sensitive information, perhaps involving health records or the involvement of social services, housing officials or the police with a family in crisis.

1.3 Professionals working for or commissioned to work for councils, the police or health care providers such as the NHS have a legal duty to keep such information confidential. There are times, however, when they need to know about each other's involvement to make sure someone is receiving the most appropriate service or is not at risk, for example.

1.4 The tragic consequences of the failure to share crucial information between agencies have been highlighted in a number of high profile media stories. Indeed, the death of Victoria Climbie became a cause celebre, which led to an overhaul of official procedures, including more emphasis on effective information sharing.

Greater clarity

1.5 When sharing confidential information, agencies need to be clear about why and how this will happen. Many organisations have already established protocols for sharing information, sometimes in line with national standards or differing professional requirements. These organisation-specific protocols remain in force, with the Surrey's overarching Multi-Agency Information Sharing Protocol there to provide the ground rules for how they can operate together.

What is the protocol?

1.6 The Surrey Multi-Agency Information Sharing Protocol is an agreed set of principles about sharing personal or confidential information. It can also be used as a framework for sharing anonymised and non-personal data (see paragraphs 2.15 – 2.20 for more details). This enables each organisation

signed up to the protocol to understand the circumstances in which it should share information and what its responsibilities are.

1.7 It does not replace individual context specific protocols (see Appendix 6), but provides a framework within which they can all operate. The Surrey Multi-Agency Information Sharing Protocol provides both a common understanding for all the agencies in Surrey to work to, and a default process for those organisations without their own specific protocol. See section 2.36.38 for further details on the MAISP user group.

2 THE SURREY MULTI-AGENCY INFORMATION SHARING PROTOCOL (MAISP)

Introduction

2.1 The principles set out in the protocol are based on good practice and the legal and professional requirements relating in particular to Surrey's public bodies. They are summarised under the Golden Rules and then explained in greater detail with supporting information and guidance in the rest of the document, including the appendices section.

Golden Rules

1. Confirm the identity of the person you are sharing with

2. Obtain consent to share if safe, appropriate and feasible

3. Confirm the reason the information is required

4. Be fully satisfied that it is necessary to share

5. Check with a manager/specialist or seek legal advice if you are unsure

6. Don't share more information than is necessary

7. Inform the recipient if any of the information is potentially unreliable

8. Ensure that the information is shared safely and securely

9. Be clear with the recipient how the information will be used

10. Record what information is shared.

Overview

2.2 The Surrey Multi-Agency Information Sharing Protocol (MAISP) is an agreed set of principles and standards under which partner organisations will share personal or confidential information, including information about people who have died, and sensitive aggregated data.

2.3 The Surrey MAISP will help the exchange of information between agencies conducting business for any appropriate purpose.

2.4 The Surrey MAISP should be applied while following established and agreed processes within the signatory organisations.

2.5 The Surrey MAISP does not give agencies an automatic right to receive information or a mandate to provide information, but is instead a process for information sharing in cases in which it is suitable for information to be shared.

2.6 The Surrey MAISP is the over-arching protocol that works with a two-tier framework for information sharing in Surrey:

Tier 1 – The Surrey MAISP - is the common set of principles and standards under which partner organisations will share information. It records the commitment of Senior Officers in each participating organisation to meet agreed standards for the sharing of personal identifiable information. The Surrey MAISP ensures that these standards are consistent across context specific Information Sharing Protocols (ISPs) and supports the drafting of more concise and easy to use ISPs.

2.7 Tier 2 - Context Specific Information Sharing Protocols

A Tier 2 ISP identifies the operational data requirements to be shared for specific and lawful purposes; essentially the "who/why/where/when/what/how" questions of sharing personal information.

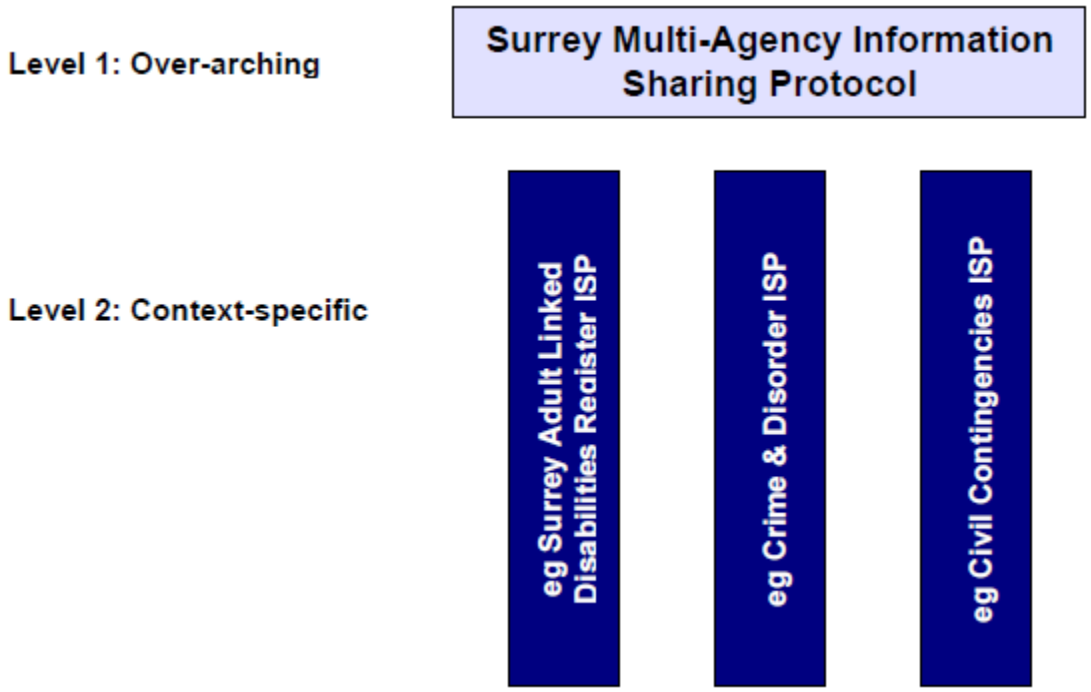
Surrey will only have one MAISP, but there will be many ISPs, for example the Crime and Disorder ISP. The MAISP contains a default ISP procedure that can be used in situations where a context specific ISP has not been defined.

The Surrey MAISP User Group will review ISPs to ensure they are MAISP compliant and will maintain a list of compliant ISPs on the web-site**.**

http://www.surreycc.gov.uk/your-council/organisations-we-work-with/partnership-services-for-families/information-sharing-for-professionals/information-sharing-protocol-for-multi-agency-staff

2.8 Level 2 ISPs should contain the following text and diagram to explain the structure:

This information sharing protocol is a context specific ISP within Surrey's information sharing framework. This information sharing protocol is compliant with the general principles for information sharing set out in Surrey's Multi-Agency Information Sharing Protocol (MAISP). Organisations that sign up to this information sharing protocol are therefore bound by the principles of the Surrey MAISP, the over-arching protocol, and are automatically signed up to the Surrey MAISP.



Please see **Appendix 6** for further information on Context Specific Protocols

Agreement

2.9 By signing up to the Surrey MAISP, signatory organisations are committed to a positive approach to information sharing.

2.10 Signatories agree to meet the commitments outlined in the body text of the Surrey MAISP in all instances of information sharing. (see Appendix 4)

2.11 Signatories will follow the default processes in **Appendix 4** where there are no other more appropriate context-specific protocols in place.

Benefits of information sharing

2.12 The imperative to share information is increasingly recognised, particularly in reducing risk to vulnerable individuals and to underpin effective partnership working. Further details can be found in the ICO's Data Sharing Code of Practice. The anticipated benefits can be summarised as:

- Better informed decision making
- Improved inter-agency working
- Better profiling of individual need or risk
- More effective intervention, support and targeting of resources
- Improved protection of individuals at risk
- Reduction in acute need through earlier effective action

Legal and statutory framework

2.13 There are many pieces of legislation that control the exchange of information in the fulfillment of public sector responsibilities. These can be found in Appendix 1.

2.14 Numerous other pieces of legislation also bestow a power or a duty on public authorities to share information in specific circumstances. All information sharing must be conducted in accordance with a relevant legal power or duty.

Definitions

Confidential information

2.15 Confidential information is covered by the Common Law Duty of Confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

Personal information

2.16 'Personal data' is defined under the Data Protection Act 1998 as anything that relates to a living individual in which the individual can be identified:

- Directly from the information (e.g. name and address), or
- From the combination of this information with other information that may be readily accessible (e.g. address but not name), and
- Which affects the privacy of the subject, whether in personal, family, business or professional life.

2.17 'Sensitive personal information' is defined under the Data Protection Act 1998 as any personal data relating to:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- membership of a trade union
- physical or mental health or condition
- sexual life
- the commission or alleged commission of any offence
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Information about someone who has died

2.18 The Data Protection Act 1998 does not apply to information about people who have died. However, it is important to note that confidentiality still exists after death and that such information may still be sensitive, confidential or relate to individuals who are still alive. It may also be covered by other appropriate legislation, such as the Access to Health Records Act 1990. Information about people who have died must still be shared under the provisions of the Surrey MAISP.

De-personalised and aggregated information

2.19 Where de-personalised or aggregated information is no longer sensitive or identifiable it may be shared outside of the scope of this protocol. Where de-personalised or aggregated information may still be sensitive (eg as a result of complexity, currency, potential for misinterpretation or misuse) it must still be treated with care under the provisions of the Surrey MAISP.

2.20 For the purposes of conducive partnership working, a Tier 2 protocol template can be used to form a basis for the sharing of anonymised or psydonymised information. Agencies are advised to refer to the Information Commissioner's Anonymisation Managing Data Protection Risk Code of Practice.

Signatories' commitments under the Surrey MAISP

Signatories are committed to:

2.21 Abiding by the Golden Rules for information sharing in all instances of information exchange.

2.22 Sharing information in accordance with the law.

2.23 Sharing information responsibly and in accordance with professional and ethical standards. See **Appendix 2**.

2.24 Sharing, receiving and storing information securely. See **Appendix 3** for guidance on information security.

2.25 Establishing realistic expectations from the outset regarding the reasons for which the information is required and the purposes for which it will be used. Recording information exchanges and refusals in such a way as to provide an auditable traceable organisational record. See **Appendix 8** for sample template forms that may be used to facilitate this.

2.26 Consulting with originating organisations before using information received under this protocol for any purpose other than that originally communicated when the information was received. This includes responding to requests for access to information from the public, as consultation is necessary for advice on sensitivities, legitimate exemptions or interpretive advice.

2.27 Signatories are not obliged to consult where they are under a legal obligation to share the information and any delays would result in serious harm. In such circumstances, signatories must inform the originating organisation as soon as is practicable.

2.28 Meeting the requirements outlined in **Appendix 5**.

2.29 Raising awareness of the Surrey MAISP within their organisation and training staff to use the protocol.

Data sharing processes

2.30 Guidance on the default process under the Surrey MAISP for the exchange of information can be found in **Appendix 4**. This guidance distinguishes between the two principal types of information enquiry:

- simple enquiries
- complex enquiries

2.31 Where Tier 2 processes for sharing information have been established in your organisation for a particular context or purpose, these should always be used rather than the default process for information exchange. Examples of context specific information sharing protocols are available via the web-site**.**

http://www.surreycc.gov.uk/your-council/organisations-we-work-with/partnership-services-for-families/information-sharing-for-professionals/information-sharing-protocol-for-multi-agency-staff

Commencement of this agreement

2.32 This agreement took effect from 31 March 2008 and was reviewed and republished in 2014. Organisations can join the protocol by completing the Sign-up Form (see **Appendix 8**) and sending a copy to The Chair of the Surrey MAISP User Group, based at Surrey County Council. Version 5.0 replaces all previous versions as the approved document all signatories should adhere to.

Review and updating

2.33 Review of the Surrey MAISP will be completed every 3 years by the Surrey MAISP user group and will be undertaken no later than three months before this deadline by a representative group of signatory organisations invited to participate based on expressions of interest.

2.34 Wider consultation will be undertaken on any proposed changes to the Surrey MAISP.

2.35 This timetable may need to be adjusted in respect of significant legislative changes, the pressure of user feedback on processes or changes in context and circumstances.

Surrey MAISP User Group

2.36 Surrey MAISP user group is made up of representatives of signatory organisations. They will provide ongoing advice, feedback and share best practice on practical issues around the application of this protocol to improve partnership working.

2.37 The group will be responsible for approving Tier 2 protocols as and when necessary.

2.38 As Surrey County Council is the lead agency, this authority will chair the group and be responsible for convening meetings, develop the web-site and be the main point of contact.

Complaints and breaches

2.39 Surrey County Council, as the lead agency, cannot be held responsible for breaches of the Surrey MAISP or complaints arising from breaches.

2.40 Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents.

2.41 Breaches of the Surrey MAISP must be dealt with by the signatory organisation under their own established policies and procedures.

2.42 A signatory that receives a complaint regarding any aspect of this protocol must process it in accordance with their organisation's established complaints policies and procedures.

2.43 The disclosing agency is responsible for accuracy of the information, and must inform the receiving agency of any subsequent changes to the information.

2.44 The MAISP User Group will take an overview of breaches/complaints and actions arising. The following types of incidents will be discussed:

- refusals to disclose information
- conditions being placed on disclosure
- delays in responding to requests
- disclosure of information to members of the staff who do not have a legitimate reason for access
- non-delivery of personal information
- disregard for procedures
- the use of data/information for purposes other than those agreed in the protocol
- inadequate security arrangements

2.45 In the event of a complaint regarding an alleged unauthorized disclosure or use of personal information that has been supplied/obtained under the information sharing process, all parties to the agreement will provide cooperation and assistance in the investigation and resolution of the complaint.

Monitoring and Audit of Tier 2 Protocols and information sharing processes

2.46 All agencies must keep appropriate records or implement systems that are capable of monitoring the operation of individual information sharing protocols. This will facilitate periodic retrospective assessment and audits to be made of whether the information sharing achieves its objectives and where it is determined that it failed to do so, the information sharing should cease or be modified as appropriate.

2.47 Audit of Tier 2 protocols and practices can be undertaken on request to the Chair of the Surrey MAISP. The primary purpose of the audit process would be to strengthen the way the principles of the MAISP are being used and then recommend where best practice can be adopted and improved.

3. Appendix 1: The Legal Framework and Supporting Guidance

The Legal and Statutory Framework

3.1 The following include but are not limited to the principle laws, guidance and regulations concerning the use of personal data :

Local Government Acts 1972 and 2000
Computer Misuse Act 1990
Childrens Acts 1989 and 2004
Data Protection Act 1998
Human Rights Act 1998
Crime and Disorder Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Regulation of Investigatory Powers Act 2000
Police Reform Act 2002
Criminal Justice Act 2003
Civil Contingencies Act 2004
Mental Capacity Act 2005
Police and Justice Act 2006
Children and Young Persons Act 2008
Localism Act 2011
The Protection of Freedoms Act 2012
Welfare Reform Act 2012
Common Law Duty of Confidence
Caldicott Principles
Safeguarding Adults, ADSS 2005
Working Together to Safeguard Children 2013 Statutory Guidance
Local Government & Public Involvement in Health Act 2007
No secrets, Department of Health 2000
Health & Social Care Act 2012

As well as the above legislation there are also a number of Codes of Practice that provide useful guidance e.g. ICO Data sharing Code of Practice, NHS Confidentiality Code of Practice etc.

Consent and capacity to share

3.2 Confidential or personal information may be shared if consent to share has been given by the confider or data subject. This should be sought if it is safe, appropriate and feasible to do so.

3.3 Where the confider or data subject does not have capacity to give consent

to share, consent may be sought from someone who may appropriately act on behalf of the data subject, for example an appropriate adult or someone who holds a relevant Power of Attorney. Relevant legislation may apply and includes, but it is not limited to the Mental Capacity Act 2005.

3.4 If it is not possible or safe to obtain consent; consideration should be given as to whether it is necessary/ appropriate to share without consent. This decision should be made in line with local signatory policy and procedures.

Recording and reviewing consent

3.5 A record should always be made of any consent that has been given or refused. This should be referred to when information is shared to ensure that the scope of the consent is not exceeded. Consent should be obtained every time the information is to be used for a different purpose to that recorded or if there has been an unreasonable lapse of time since consent to share was given.

Informed consent

3.6 Consent must always be informed. This means that the person or the authorised representative giving consent must clearly understand all the available options and the consequences of them giving their consent.

Explicit or express consent

3.7 This is a clear and voluntary indication of consent to share specific information for one or more specified purposes.

Implied consent

3.8 This applies where it would be within the reasonable expectations of the data subject or confider that information may be shared without needing to obtain explicit consent. It is likely to apply where information is routinely shared and the data subject is aware of this or where information sharing is intrinsic to the purpose for which the data subject or confider supplied the information.

Withdrawal or reconfirmation of consent

3.9 The confider or data subject may withdraw consent at any time and they should be made aware of this right. If consent is withdrawn, others with whom the information has been shared must be notified.

3.10 Consent must not be assumed to be open-ended. Confirmation of continued consent should be sought after a reasonable time according to individual circumstances and an expiry date for consent should be recorded.

3.11 In the event of a change in either the extent of information being sought, or the need to share with agencies not included in the original consent agreement, a revised consent should be sought unless the information may legitimately be shared without consent.

Sharing information without consent

3.12 It is not always safe, appropriate or feasible to obtain consent to share information. Circumstances where it may not be possible to obtain consent include:

- Where obtaining consent might be contrary to the public interest
- The data subject / confider may be absent or not contactable
- The data subject / confider may be permanently or temporarily incapacitated and has no appropriate representative
- The data subject / confider has withheld or withdrawn their consent
- Where the data subject is deceased

3.13 Under the Common Law Duty of Confidence, the Data Protection Act 1998 and the Human Rights Act 1998 it is possible to disclose information without consent in the cases of serious public interest or in the best interests of an individual. Decisions regarding the disclosure of information without consent must be made on a case-by-case basis. Any disclosure must always be proportionate and the minimum necessary to achieve the necessary objective.

3.14 If it is not possible to obtain consent before sharing information, the data subject / confider should be informed as soon as possible after the information has been shared, unless this would be inappropriate.

3.15 It is important that information about identifiable individuals should only be disclosed on a strict need to know basis and in keeping with the Surrey Multi-Agency Information Sharing Protocol of which this Appendix is a part. Strict controls governing the disclosure of patient identifiable information are also a requirement of the Caldicott recommendations.

3.16 Some disclosures of information may occur because there is a statutory requirement upon the organisation to disclose e.g. with a Court Order, because other legislation requires disclosure.

Best interests

3.17 Where an individual is unavailable or does not have capacity to consent to the sharing of information, they may have an appointed representative or other person working with them. A decision should be made in the best interests of that individual.

The impact of sharing or withholding information

3.18 Essentially, a decision to share information without consent rests on an assessment of the relative risk of disclosure and non-disclosure and a professional judgment on the most appropriate action that should be taken in the light of this assessment.

3.19 Two key questions are:

1. What could happen if this information is not shared?
2. Who will be affected by this information being shared?

3.20 The former considers whether a negative impact is likely if the information is withheld. There will be a clear interest in disclosing information where there is an evident risk to the life or well-being of an individual which is accentuated or not addressed by not doing so; the protection of health, morals and the rights and freedoms of others; public safety; and the prevention of crime and disorder. If substantive, the public interest value may over-ride that of an individual's human rights.

3.21 The latter considers whether there is a disproportionately negative impact in information being made available, for example familial breakdown or personal risk resulting from unnecessary disclosure. Disclosure should be assessed for its potential impact on others who may be identifiable from the data (such as witnesses, or staff who are involved in cases) or whose vulnerability makes their interests the over-riding consideration (such as children at risk).

The Common Law Duty of Confidentiality

3.22 Confidential information is covered by the Common Law Duty of Confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

3.23 The key principle is that any information confided should not be used or disclosed further except as originally understood by the confider or with

their subsequent permission.

3.24 The duty is not absolute and the disclosure of confidential information can be justified if:

- the information is not confidential in nature
- the person to whom the duty of confidence is owed has expressly authorised its disclosure
- disclosure is required by a court order
- disclosure is required by legislation or a legal obligation
- there is a serious overriding public interest.

The Data Protection Act 1998

3.25 Personal data is defined under the Data Protection Act (1998) as anything that relates to a living individual in which the individual can be identified:

- directly from the information (eg name and address), or
- from the combination of this information with other information that may be readily accessible (eg address but not name), and
- which affects the privacy of the subject, whether in personal, family, business or professional life (ICO guidance on definition of personal data).

3.26 Sensitive personal information is defined under the Data Protection Act (1998) as any 'personal data' relating to racial or ethnic origin; political opinions; religious or similar beliefs; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence; any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Sharing personal and sensitive personal data

3.27 The Eight Data Protection principles listed under Schedule 1 of the Data Protection Act (see **Appendix 2**) must be complied with when processing any personal or sensitive personal data, unless an exemption applies.

3.28 One of the conditions listed under Schedule 2 of the Data Protection Act 1998 must be met before any personal or sensitive personal data can be shared, unless an exemption applies.

3.29 Before sensitive personal data can be shared, one of the conditions from Schedule 3 of the Act must be met in addition to one of the conditions from Schedule 2, unless an exemption applies.

To see the Data Protection Act 1998 in full, please visit the official UK

legislation website: **www.legislation.gov.uk**

Human Rights Act 1998

3.30 Public authorities must share information in accordance with the Human Rights Act 1998, which states that everyone has a right to respect for private and family life, his home and his correspondence.

3.31 A public authority may share information which may interfere with the above right if to do so is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country for the prevention of disorder or crime, protection of health or morals or for the protection of rights and freedom of others.

Freedom of Information Act 2000

3.32 A number of partner agencies are 'public authorities' for the purposes of the Freedom of information Act 2000 (FOI). This means that they could receive requests for information relating to information sharing activities. It is recognised that public authorities are individually responsible for meeting their FOI Act obligations.

3.33 Under the FOI's section 45 Code of Practice on handling requests for information, good practice is to consult with third parties who have given information which may be disclosed under the FOI Act, therefore and if it is deemed to be appropriate, care should be taken by the public authority receiving the FOI request to ensure that partner agencies are informed in a suitable manner of the nature of the request and their intended response.

This is summary guidance of the key legislation and principles current to this revised edition of the MAISP 2014. Legal or specialist advice should be sought for greater detail, clarity or advice on specific situations.

4. Appendix 2: The Eight Data Protection Principles and Professional Standards

4.1 All signatories to the Surrey Multi-Agency Information Sharing Protocol are required to abide by the principles laid down in the Data Protection Act 1998. However, most organisations will also be required to observe professional standards (such as the Caldicott Principles).

4.2 Below is a list of the principles. There is extensive guidance for each of the principles on the ICO's website.

The common rules that all signatories must abide by are the eight principles outlined in Schedules 1 and 2 of the Data Protection Act 1998.

Principle 1: Personal data shall be processed fairly and lawfully

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

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

Principle 4: Personal data shall be accurate and, where necessary, kept up to date

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act

Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

5. Appendix 3: Data Exchange, Security and Disposal

5.1 The Data Protection Act principles (see **Appendix 2**) require that data is exchanged, held and disposed of within an effective security framework. **It is recognised that organisations will work to their own policies and guidance on this subject matter and the following is a useful training tool for agencies to use as practical examples of methods of exchange.**

Data exchange and security

5.2 **Appendix 4** provides specific guidance on the recommended processes for data exchange, together with sample forms. Underpinning this is a set of general principles relating to sensitive personal data to be used if a specific Information Sharing Protocol does not exist.

5.3 At all stages of the exchange the principle that the information should be available only to those who have a specific and legitimate need to see it must be maintained by both the sender and the recipient.

5.4 Documents and information exchanged should be protectively marked where a scheme has been adopted by an organisation; this is to ensure that the person receiving the information can adopt suitable security measures to prevent the information from being compromised or unlawfully disclosed. For example, some public sector organisations use the Government Protective Marking Scheme.

5.5 Data must only be sent if the means of transmission is secure and it can be established that the appropriate recipient's access to the transmission is equally secure.

5.6 Data must be stored securely, regularly reviewed and disposed of in accordance with the receiving organisation(s) Retention and Disposal policy and procedures when no longer required for the purpose it was originally obtained.

5.7 The Surrey Multi-Agency Information Sharing Protocol is based on the principle that sharing of personal data between agencies is done on an individual case-by-case basis. However, it may be necessary for organisations or agencies to transfer data in bulk or in batches. Where required some agencies may prefer to sign a bulk data transfer or other specific agreement on how the information is transferred. To ensure the security of this data, controls must be in place to secure the data during transit and when received. Such transfers must be compliant with the sending organisation's security policy or guidance and agreed by the receiving organisation whether paper documents or records or electronic

data (e.g. encryption of all personal identifiable data held on portable media such as, laptops, memory sticks).

Secure information exchange methods

5.8 It is important that information is shared safely and only shared with the intended recipient. The information should show the originator's details, including organisation name (if applicable) and date. Information can be shared in a variety of ways and there are advantages and disadvantages to each method. The ways in which you may choose to exchange information are set out below.

5.9 E-mail

Please note that emails across the public internet are not secure. If you intend to use email for data exchange you must add appropriate security such as encryption. Seek advice from your organisations information security advisor.

5.10 Fax

Faxing is not considered a secure method of sending personal information as has been illustrated by the fines placed on various organisations by the ICO. It is recommended that a fax protocol is set up to ensure security is maintained.

5.11 Postal or Courier Services

It is recommended that if you use postal services you minimise the risk of loss. An example is to put the information in one envelope marked private and confidential and place in another envelope addressed to an individual. It is recommended that if the Post Office system is used, Recorded Delivery or Registered Delivery is chosen, as this allows the mail to be tracked. A courier service could alternatively be used, depending on the sender's requirements or sensitivity of the information.

5.12 Personal exchange

Paper copies of information can be exchanged in person provided that both the information holder and the recipient take appropriate measures to ensure that they cannot be read by anyone who does not have a legitimate reason to do so. Paper copies should be kept secure at all times. Ensure the recipient is the correct recipient.

5.13 Verbal exchange

Before you are exchanging information be sure that you are talking to the person who is entitled to the information. A verbal exchange is only secure if it is not repeated to anyone who is not authorised to hear it, or overheard when exchanged or discussed (e.g. in a busy office or during a conference phone call). If information is exchanged verbally in a manner where it is not recorded at the time, the exchange should be validated and confirmed in writing as soon as possible. With the sharing of premises, verbal exchange between organisations has become prevalent. You will need to make sure any exchange is done so in a formal manner and is recorded appropriately.

5.14 Conference

Much information sharing will take place in confidential conference meetings to determine a course of action in respect of specific named individuals and to which appropriate individuals are invited. Exchange may be oral or on paper but data protection principles must still apply with attendees only being present where it is appropriate for them to share the information. A form to enable a single declaration relating to the meeting's business is included in **Appendix 8**. Information exchange that takes place at the meeting should be recorded and validated in the full minutes.

Data retention and disposal

5.15 The length of time that exchanged information is retained will need to be determined on a case by case basis, but always in compliance with the requirement that it is only kept for the minimum period necessary ***to achieve the specific aims for which it was obtained***. After this, the information must be returned to the owner or destroyed, as agreed.

5.16 Both the requesting and the supplying agency should keep a copy of any records relating to information exchanged .This should be kept in accordance with the organisation's policies on retention and disposal. Commercially sensitive or personally identifiable data must be securely destroyed.

5.17 Physical copies of information should be shredded when they are no longer required. Electronic copies should be "double deleted" i.e. not just from the disk or server, but also from any back-ups that are retained.

6. Appendix 4: Processes and Designated Officers

This process should only be used if an alternative protocol is not available in a specific context. Sample forms are attached at Appendix 8 and may be used as templates only. Please contact your Information Sharing Lead for guidance for your own organisation's forms, or see the web-site for examples of context specific protocols.

This protocol has identified two principal types of enquiry:

Simple enquiry

6.1 These are restricted to the confirmation that information is available on a specific individual or issue. This process confirms that information is held, but does not involve any further exchange of detail:

- An agency signed up to the Surrey MAISP enquires, verbally or in writing, whether your agency holds information on an individual.
- If the answer is no then you should inform the agency.

Complex enquiry

6.2 If the answer is yes, and the agency wants more information, this process then becomes a Complex Enquiry, which is any exchange that involves the transfer of detail beyond that covered by the simple enquiry. You should tell the agency that if they wish to apply for more information they should complete **Form 1,** or **Form 3 (see Appendix 8)** if the consent of the individual has been obtained to release this information. The process is as follows:

6.3 Once the **Form 1** or **Form 3** has been received, if your agency has a Designated Officer or similar, refer the enquiry to them.

6.4 If this is not practicable and would unnecessarily delay the response then complete the recipient box on the bottom of **Form 1** and indicate whether the information will be shared.

6.5 If the information requested will not be released then reasons for this must be stated on the **Form 1** and a copy returned to the requesting agency.

6.6 If the information requested is to be shared then it should be shared promptly by the most appropriate secure medium (see **Appendix 3)**.

6.7 In all cases the original **Form 1** or **Form 3** should be retained, with a record of what information has been shared and with whom.

6.8 Where Designated Officers or similar exist within an organisation they should be made aware of any information exchange via **Form 1** or **Form 3** for audit purposes.

6.9 All information requests must be responded to promptly and preferably within 5 working days of receipt. If the agency requesting has an urgent timescale that needs to be met, they should make this clear to the agency that holds the information.

Multi-Agency meetings

6.10 Information exchange will also take place in meetings which are considering specific individuals or groups of individuals with a view to assessing risk, developing a fuller shared understanding of relevant issues, or developing effective responses and interventions. Information exchange in this context will usually, in the first instance, be oral but must still be governed by data protection and confidentiality principles. To this end such meetings should ensure that:

6.10.1 Those attending have a legitimate reason to be part of the process, either as information sharers or decision makers.

6.10.2 The agenda structure should enable attendance for only part of the meeting where a number of cases are reviewed but are not relevant to all.

6.10.3 The individuals under consideration should normally be made aware of this process and, where appropriate should be invited to attend. There will be circumstances however where it will not be appropriate for the individuals to be made aware of the process. Where this is the case, the reasons should be stated at the start of the meeting.

6.10.4 Data protection and confidentiality principles should be confirmed at the beginning of each meeting. A signatory form such as **Form 2** should be signed by those attending and kept as part of the record of the meeting

6.10.5 The meeting record and any associated paperwork will be managed in accordance with data security principles as set out in **Appendices 2 and 3**. Any information or records shared outside of the group should be suitably depersonalised, or appropriately targeted.

Roles and Responsibilities

Information Sharing Leads

6.11 The Surrey MAISP User Group will maintain a list of contact details for Information Sharing Leads and, where appropriate, Caldicott Guardians, for all organisations signed up to the Surrey MAISP. Signatory Organisation's names will be published on the Surrey MAISP website.

6.12 Organisation Sharing Leads will:

6.12.1 Contribute to reviews of the Surrey MAISP or related processes as required.

6.12.2 Ensure that the Surrey MAISP requirements are reflected in training, data security or management and complaints processes.

6.13 Signatories may choose to assign specific staff to facilitate, manage or advise on information sharing as appropriate for their organisation. These may be existing data protection, information security or information governance staff. Alternatively, signatories may choose to identify specific officers/staff responsibilities for information sharing.

6.14 Signatories may choose for all or most information sharing to be channeled through Designated Officers or they may decide that it is more practicable for Designated Officers to take a consultative role, advising staff on information sharing when required.

7. Appendix 5: Signatory Organisations Requirements and Responsibilities

Signatories are responsible for ensuring that their organisations are complying with the legislative framework behind this Protocol and working with policies that adequately reflect the secure processing of data.

Signatories to this protocol must be able to respond positively or work towards all of the following requirements.

Requirement Level

		Working towards
	We have an information security policy	
	We have a Data Protection policy	
	Notification to the Information Commissioner's Office is up to date	
	An Information Sharing Lead or other nominated individual with these responsibilities has been appointed and are known to staff	
	Information Security Training is provided to all staff including those who are permanent, temporary, voluntary, contract, students on placements, locums, bank staff, and in any other category.	
	The organisation is aware that it will be legally responsible for the information held within the organisation as required by Data Protection legislation	
	The organisation to which information is sent is aware of the purpose for which the information was originally collected, to ensure that processing does not contravene the Data Protection Act 1998.	
	We will respond to requests for information within a reasonable time scale (as agreed in local/specific agreements and included in legislation e.g. Data Protection Act 1998)	

	The organisation has confidentiality agreements with all contractors relating to service user information.	
	Access to information is adequately controlled (passwords, network access controls, physical security measures etc)	
	All new information systems should be designed to include clear audit trails for all access/uses of towards information	
	All remote accesses to networks are provided by a secure virtual private network or similar	
	All information sharing will be recorded to provide auditable records as well as for the immediate purpose	
	We have safe environments for sending and receiving personal information and have procedures for their use	
	Records are kept, and disposed of, in accordance with local and national policies and guidelines.	
	All portable equipment containing person identifiable service user information is encrypted in accordance with best practice as advised by the ICO.	

8. Appendix 6: Context Specific Protocols – Tier 2

The Surrey Multi-Agency Information Sharing Protocol can be used by any organisation as a default protocol. Where a context specific protocol is in place (known as a Tier 2), this should be used in place of the Surrey MAISP.

These Tier 2 detail:

- the specific purpose(s) for information sharing
- the group(s) of service users it impacts upon
- the relevant legislative powers and the consent processes involved
- what data is to be shared
- the required operational procedures and the process for review
- the means of communicating to practitioners the specific operational requirements

Guidance on how to create a Tier 2 Protocol can be found on the web-site.

http://www.surreycc.gov.uk/__data/assets/pdf_file/0006/173508/MAISP-Compliance-Template.pdf

Tier 2 Protocols that are Surrey MAISP compliant can be found on the web-site.

http://www.surreycc.gov.uk/your-council/organisations-we-work-with/partnership-services-for-families/information-sharing-for-professionals/information-sharing-protocol-for-multi-agency-staff

Please note there is a central government protocol in place for emergencies and responding to major incidents.

9. Appendix 7: References

ICO web-site address:

http://www.ico.org.uk/

ICO Data Sharing Code of Practice and checklists:

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Lord Chancellor's Code of Practice on Records Management:

http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

IRMS Local Government Classification Scheme:

http://www.irms.org.uk/resources/information-guides/198-local-government-classification-scheme-v203

MAISP Leaflet:

http://www.surreycc.gov.uk/__data/assets/word_doc/0018/171207/MAISP-Leaflet.doc

10. APPENDIX 8: SAMPLE FORMS

Sample Form 1: Request for Personal Information

Form for requesting personal or sensitive personal information from another agency.

Part 1: to be completed by the agency requesting information

Personal details of the subject of the information [Only include enough detail as is necessary for the recipient to identify the subject]			
Our reference:		Last Name:	
First Name:		Any previous surnames:	
Also known as:		Date and place of birth:	
Current address: Postcode:		Previous address: (if known)	
Scope and reason for the request			
Information required:			
Data Protection Act justification for disclosing this information:			
Purpose for which this information is required:			
Consequences of failure to provide information:			
Signed		Date	
Name		Job title	
Agency			

Part 2: to be completed by the agency that holds the information

Information supplied?		Yes / No [delete as applicable]	
If no, reason for refusal:			
Signed		Date	
Name		Job title	
Agency			

We, the signatories, understand, that this request for information has been made according to the principles of the Surrey MAISP and that the information shared as a result is for the specific purpose stated.

Under the principles of the Surrey MAISP, both the requesting and the supplying agency should keep a copy of any records relating to information exchanged in line with their organisation's policies. The information will be stored securely and not shared outwardly without the express consent of the originating body.

Sample Form 2: Information in Multi-Agency Meeting

Declaration of agreement to information sharing principles for use in confidential meetings	
Meeting title:	
Purpose of meeting:	
Date:	

We, the undersigned, accept and understand that the principles of the Surrey Multi-Agency Information Sharing Protocol and the legislation regulating the exchange of information apply to the content of this meeting. We understand that information shared and exchanged at this meeting is for the specific purpose identified above.

Name	Organisation	Signature

1. Those attending have a legitimate reason to be part of the process, either as information sharers or decision makers.
2. If necessary the agenda structure should enable attendance for part only of meetings where a number of cases may be reviewed but are not relevant to all.
3. The individuals under consideration should normally be made aware of this process and, where appropriate, should be invited to attend. However, in some circumstances it will not be appropriate for the individuals to be made aware of the process.
4. Data protection and confidentiality principles should be confirmed at the beginning of each meeting.

This form will be retained as part of the meeting record. Please file this form with a copy of all information shared attached to it. Under the principles of the Surrey MAISP each agency should keep a copy of any records relating to information shared in line with their organisation's policies. The information will be stored securely and not shared outwardly without the expressed consent of the originating body.

Sample Form 3: Permission to Share Personal and Confidential Information

Form to indicate consent to share personal and confidential information

Our reference	

1. Your details			
Last Name:			
First Name :			
Address including postcode:			
2. Who we are (Organisation and contact details)			
3. Your personal and confidential information that we wish to share			
4. The people with whom we want to share this information (please indicate if you do not want us to share with any of those listed)			
5. The reason we want to share it			
6. Declaration			
I give you permission to share my personal and confidential information as described in section 3, with the people indicated in section 4 and for the purpose described in section 5. I understand that I may withdraw my consent at any time at the address given in section 2.			
Signed		Date	
7. To be signed by the person requesting consent			
Signed		Date	
We will only use the information on this form for the purpose mentioned. We cannot use it for any other purpose, unless you have given us permission.			

This form will be filed with a copy of all information shared attached to it. In line with the principles of the Surrey Multi-Agency Information Sharing Protocol, each agency will keep a copy of any records relating to information shared in line with their organisation's policies.

Sample Form 4: Surrey MAISP Sign Up Form

The Surrey Multi-Agency Information Sharing Protocol is intended to facilitate the exchange of personal or sensitive information between signatories for any appropriate purpose.

Signatories to this protocol agree to the signatories' commitments, and understanding of the requirements outlined in Appendix 5. They commit to a positive and legal approach to information sharing, as defined in this document. This protocol will be reviewed at least every three years.

Signatories:

Organisation
Chief Executive (signature and print name)
Information Sharing Lead, eg Data Protection Manager (print name and job title)
Caldicott Guardian (print name and job title)
ICO Notification Number
Date

When completed, please send a copy of this form to:

Chair of Surrey MAISP User Group
C/o Corporate Information Governance Manager
Legal & Democratic Services
Surrey County Council
County Hall, Penrhyn Road
Kingston upon Thames
KT1 2DN