



Whole Essex Information Sharing Framework

This Information Sharing Protocol is designed to ensure that information is shared in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

This protocol will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits include:

- transparency for individuals whose data you wish to share as protocols are published here;
- minimised risk of breaking the law and consequent enforcement action by the Information Commissioner’s Office (ICO) or other regulators;
- greater public trust and a better relationship by ensuring that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- increased data sharing when this is necessary and beneficial;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people’s knowledge or consent or in the face of objection; and reduced risk of questions, complaints and disputes about the way you share personal data.

Please ensure all sections of the template are fully completed with sufficient detail to provide assurance that the sharing is conducted lawfully, securely and ethically.

Item	Name/Link /Reference	Responsible Authority
Privacy Impact Assessment		
Supporting Standard Operating Procedure		
Associated contract		
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the [WEISF Portal](#).

INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement		Overarching Safeguarding agreement		
Organisation Name	Head Office Address	Telephone	Email	ICO Registration reference
Essex County Council	County Hall. Chelmsford. Essex. CM1 1QH	08457 430430	Informationgovernanceteam@essex.gov.uk	Z6034810
			See Appendix D for all signatories	
Version Control				
Date Agreement comes into force	01/04/17			
Date of Agreement review	24/05/18			
Agreement owner (Organisation)	Essex County Council			
Agreement drawn up by (Author(s))	Kellene Green			
Status of document – DRAFT/FOR APPROVAL/APPROVED	APPROVED			
Version	V4.0			

Information Sharing Protocol – Overarching Safeguarding Agreement

1. Purpose

Living a life that is free from harm and abuse is a fundamental right of every person. All the signatories to this agreement are at the forefront of preventing harm or abuse and taking action where necessary. Abuse is a violation of an individual's human and civil rights by any other person or persons.

The purpose of information sharing under this protocol is to:

- Facilitate the exchange of personal and sensitive information in the interests of protecting children, young people and adults from actual or potential harm and to ensure that when information is shared the legal means to do so exist.
- Provide early and effective multi-agency intervention to safeguard **children and** adults with care and support needs, which will promote social inclusion, health and well-being.
- To encourage and help develop effective information sharing between different services and professional groups, based upon trust and mutual understanding
- Facilitate and provide clear guidance on the exchange of personal and sensitive information for the investigation and response to suspected abuse and neglect of **children and** adults within Essex, **under the Safeguarding Adults and Children procedures**

[SET Safeguarding Adult Guidelines](#)

[SET Safeguarding and Child Protection Procedures](#)

- Support the prevention and reduction of crime and identification and apprehension of offenders and suspected offenders. This will include the identification of those offenders who present a serious risk of harm to the public and ensure that appropriate plans are drawn up and implemented to manage the risk the offenders present, thereby protecting victims and the public to meet statutory requirements.

The underpinning values for sharing information under this protocol are:

- Safeguarding and promoting the welfare of children and adults with care and support needs is the prime consideration in all decisions about whether to share information.
- Professionals can work together effectively to safeguard and promote the welfare and well-being of children and adults only if there is an exchange of relevant information between them.

- Where an adult with care and support needs has a need for services from a number of agencies, ongoing appropriate information sharing between those agencies is likely to be necessary.
- Workers should share only as much information as they need to – but should share enough to achieve the purpose for which information is being shared.

The consent of those involved to share information should be obtained unless it would place someone at risk or be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders (See Appendix A). The competence of an adult to understand the issues must be considered when seeking consent (see appendix A).

Personal information relating to a child or adult is private to them and should generally be kept confidential. People should normally be kept aware of what is happening to information relating to them and have the right of access to it unless it would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution

Article 8 of the European Convention on Human Rights gives everyone the right to respect for their private family life, home and correspondence. Authorities may only interfere with this if they are not doing anything which is against the law, have a legitimate purpose (including protection of health and the rights of others), and the action is no more than is needed. Sometimes this may mean a worker has to judge one person's rights against another's or the different rights of one person (for example, an adult's right to privacy against their right to protection).

2. Information to be shared

We will share any information relevant to safeguarding as allowed by legislation. The following are examples of the information to be shared, **but it should be noted that the sharing relates to all multi-agency safeguarding groups, and not only those noted below.** Specific information to be shared in particular groups will be included in individual Standard Operating Procedures (SOPs) under Appendix E.

- Service user's name, address, age, details of racial or ethnic origin, physical and/or mental health;
- Information exchanged in the course of safeguarding both adults and children's procedures about alleged victims and alleged perpetrators;
- Data relating to an offence – nature of the offence, time, date, location of offence;
- Information that will contribute to assessment to enable workers to complete a holistic assessment of the person's needs;
- Information exchanged for the purposes of risk management via Multi-agency Public Protection Arrangements (MAPPA), such as data relating to convictions, cautions, final warnings, reprimands, details of case histories and intelligence, if appropriate and proportionate, to the subject person;
- Information about risk posed by people who are convicted of offences against children and vulnerable adults and who are potential offenders;
- Information required to manage risk and formulate safety plans for victims and their families via the Essex Safeguarding Children Board and the Essex Safeguarding Adults Board meetings;

- Information required for safeguarding reviews such as Serious Case Reviews (SCR), Serious Adult Reviews (SAR) and Partnership Learning Reviews
- Information as required for Child Death Overview Panels and the Child Death Review process
- Data required for Multi-agency Risk Assessment Conference (MARAC)
- Data required to plan for and respond to emergencies in Essex as permitted by; Regulations 45 to 54 of the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005;
- Data required to meet any inspection regimes, timescales and requests;
- Data required as part of the work on the Health and Social Care prevention agenda;
 - child's name, address, gender, date of birth, and a unique identifying number;
 - contact details for parents/carers;
 - contact details for services working with a child: as a minimum, educational setting (e.g. school) and GP practice, but also other services where appropriate;
 - Type and details of concerns and case information;
 - Details of Family Support Meetings.
- Datasets and information required for Essex Missing And Child Exploitation (MACE) groups and Child Sexual Exploitation Triage meetings. Including information on potential suspects or person/s of concern linked to child sexual exploitation and hot spots. The collation of data in the support of patterns or trends and the early identification of exploitation and trafficking.
- Information sharing to support the PREVENT Strategy.
- Information which can be used for monitoring and evaluation purposes, e.g. performance data. Where there is a risk that individuals may be identified from the data, then information will be anonymised;
- Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.
- Information to support other multi-agency groups set up to safeguard children or adults.

3. Legal Basis for sharing information

Local authority responsibilities for sharing information under the Care Act 2014

Under the Care Act 2014 a local authority must:

- set up a safeguarding board; the board will share strategic information to improve local safeguarding practice
- cooperate with each of its relevant partners; each relevant partner must also cooperate with the local authority.

Clause 45 of the Care Act focuses on 'supply of information'. This relates to the responsibilities of others to comply with requests for information from the safeguarding adult board. The statutory guidance to the Care Act emphasises the need to share information about safeguarding concerns.

If certain conditions are met, a person or body must supply information to a SAB at its request, or to any other person mentioned in the request. The information must be requested for the purpose of enabling or assisting the SAB to perform its functions. But its functions relate to doing anything it believes necessary to co-ordinate and ensure the effectiveness of all those who exercise 'enquiries' functions.

The Caldicott principles

The sharing of information in health and social care is guided by the Caldicott principles. These principles are reflected in the Data Protection Act and are useful to other sectors:

- Justify the purpose(s).
- Don't use personal confidential data unless it is absolutely necessary.
- Use the minimum personal confidential data necessary for purpose.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. This should be taken into consideration as well as the remainder of the Caldicott Principles when deciding to share personal information.

Listed in Appendix B of this document is the underpinning legislation likely to apply to sharing under this protocol.

The Children Act 1989 / 2004

The Children Act 1989 provides a comprehensive framework for the care and protection of children, centring on the welfare of children up to their 18th birthday. It defines parental responsibility and allocates duties to local authorities, courts, parents and other agencies in the United Kingdom, to ensure children are safeguarded and their welfare is promoted. The Children Act 2004 makes provision about services provided to and for children and young people by local authorities and other bodies and requires that they work together in improving the well-being of children in the local area.

The Human Rights Act 1998

- Under Article 8 of the European Convention on Human Rights, individuals have a right to respect for their private life.



- This is not an absolute right and can be overridden if necessary and in accordance with the law.
- Interference must be justified and be for a particular purpose.
- Justification could be protection of health, prevention of crime, protection of the rights and freedoms of others.
- A decision to share information and the reasoning behind it should be recorded.

The Crime and Disorder Act 1998

Any person may disclose information to a relevant authority under Section 115 of the Crime and Disorder Act 1998, 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. 'Relevant authorities', broadly, are the police, local authorities, health authorities (clinical commissioning groups) and National Probation Service and Essex Community Rehabilitation Company.

The Mental Capacity Act 2005

'Professionals and other staff need to understand and always work in line with the [Mental Capacity Act 2005](#). They should use their professional judgement and balance many competing views. They will need considerable guidance and support from their employers if they are to help adults manage risk in ways that put them in control of decision-making if possible'.

The Mental Capacity Act will apply if there is any doubt that the person concerned has the mental capacity to make specific decisions about sharing information or accepting intervention in relation to their own safety.

The Data Protection Act 1998

The Data Protection Act 1998 sets out the parameters for sharing information appropriately and safely. Any personal information should be shared on the basis that it is:

- necessary for the purpose for which it is being shared
- shared only with those who have a need for it
- accurate and up to date
- shared securely and in a timely fashion
- not kept for longer than necessary for the original purpose.

In order to comply with the Data Protection Act 1998 (DPA), one requirement is that personal information is shared fairly and lawfully (principle 1). In order to achieve this, organisations must comply with a least one condition from schedule 2 and, where sensitive information is included, at least one condition from schedule 3 of the DPA. The schedule 2 and 3 conditions can be found in Appendix C of this document.

Vital interest



'Vital interest' is a term used in the Data Protection Act to permit sharing of information where it is critical to prevent serious harm or distress, or in life-threatening situations. If the only person that would suffer if the information is not shared is the subject of that information, and they have mental capacity to make a decision about it, then sharing it may not be justified.

The [Information Commissioners Office](#) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Other legislation and guidance

- Information regarding the high risk of domestic abuse may be shared under the following legislation:
 - Children Act 1989/2004
 - Articles 2 and 3 of the Human Rights Act 1998
 - Equalities Act 2010
 - Section 115 Crime and Disorder Act 1998
 - Section 120 Learning and Skills Act 2000
 - Section 325 Criminal Justice Act 2003 (Duty to co-operate)
 - Sections 39 & 39a Police Act 1996 (Code of Practice on the Management of Police Information)
- HM Government has published an advice and guidance document which should be read in conjunction with this agreement and is an invaluable resource for all safeguarding professionals;

[Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers 2015](#)

This HM Government advice is non-statutory, and has been produced to support practitioners in the decisions they take when sharing information to reduce the risk of harm to children and young people.

- Local authorities have overarching responsibility for safeguarding and promoting the welfare of all children and young people in their area. They have a number of statutory functions under the 1989 and 2004 Children Acts which make this clear, and the guidance contained in the HM Government document [Working Together to Safeguard Children](#) sets these out in detail. This includes specific duties in relation to children in need and children suffering, or likely to suffer, significant harm, regardless of where they are found, under sections 17 and 47 of the Children Act 1989.
- A further publication, [Information Sharing to protect vulnerable children and families](#), was produced by the Centre of Excellence for Information Sharing to help the DfE, national organisations with a child protection focus and local safeguarding and early help



partnerships to understand the challenges and best practice in sharing information to protect vulnerable children and families.

- In March 2015, the Government issued a report on [Tackling Sexual Exploitation](#), along with a letter on [Our joint commitment to share information effectively for the protection of children](#).

Other relevant legislation, codes of practice and guidance are listed in Appendix B

Consent

It is good practice to seek the consent of data subjects. However, WEISF members agree that disclosure without consent is lawful if certain conditions are met. For example, personal information may be shared when anonymised or to ensure the performance of public functions or legal obligations.

Children Act 1989 Section 47 thresholds do not determine whether or not consent should be sought to request or disclose information. If professionals consider it justifiable to override the refusal of consent or the need to gain consent in the interests of the welfare of the child/young person or the vital interests of an adult then they can and must do so. This decision must be proportionate to the harm that may be caused by proceeding without consent. Such decisions must be documented by the Practitioner.

Occasionally, an individual may refuse to give consent to share their information. Where it is lawful to share such information in spite of the refusal, the data controller must record the refusal of consent and the reasons for overriding that refusal.

The data controller is responsible for ensuring that data subjects are advised when appropriate that their information is being or may be shared.

4. Access and individuals' rights

Subject Access is an individual's right to have a copy of information relating to them which is processed by an organisation.

Once information is disclosed from one agency to another, the recipient organisation becomes the **Data Controller** for that information. With regards to subject access requests, the **Data Controller** has a statutory duty to comply with section 7 of the DPA, unless an exemption applies. It is good practise for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory 40 calendar day, time period.



Subject Access requests will be dealt with by each organisation in line with their internal process and procedures. If an organisation receives a Subject Access request relating to the information held by the partner organisation, then the requester will be referred as appropriate to the correct data controller.

If a party receives a request for information under the Freedom of Information (FOI) Act 2000 or Environmental Information Regulations (EIR) 2004 that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, it is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption/exception under the provisions of the FOI Act or EIR and to identify any perceived harms. However, the decision to release data under the FOI Act or EIR is the responsibility of the agency that received the request.

FOI and EIR requests will be dealt with by each organisation in line with their internal process and procedures. If an organisation receives a, FOI or EIR request relating to the information held by the partner organisation, then the requester will be referred as appropriate to the correct data controller.

5. Keeping information secure

Security for the exchange of information will be achieved through:

- Ensuring that appropriate organisational and technical security measures are applied to all WEISF members' electronic systems that information may be transferred to
- Encryption of all portable devices to industry standard;
- Appropriately marking paper records (for example, "Official-Sensitive");
- Using agreed processes for checking the identity of the recipient;
- Applying other appropriate secure technologies.
- Robust access controls must be in place and permission to access information held will be granted on a strict 'need-to-know' basis

WEISF members receiving shared information will:

- Ensure that their workers are able to access only the shared information necessary for their role;
- Ensure that their workers are appropriately trained so that they understand their responsibilities for confidentiality and privacy;
- Protect the physical and electronic security of the shared information
- Restrict access to data to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks'
- Maintain up to date policy available to all staff for handling personal data
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents

6. Information format, method(s) and frequency of sharing

Information will be exchanged using secure methods approved by partners, e.g. *Govconnect* and these may include: verbal exchanges by telephone or face-to-face, fax, letters and other written material; secure websites and electronic records. The following general standards should be considered when exchanging information:

- Where information is exchanged via email, only secure email will be used, e.g. via Public Services Network (PSN) which includes GCSx, nhs.net, .pnn, cjsm, .gsi or a secure system such as Egress;
- When exchanging information via email, telephone, post etc. members are to ensure that their local procedures surrounding secure methods of data transfer are followed these should include the following:
 - When disclosing information by telephone consideration must be given to authenticating the caller and ensuring sensitive conversations are not overheard;
 - Do not send personal or confidential information to personal email addresses;
 - Information in hard copy format sent via Royal Mail must be double wrapped;
 - If the data is particularly sensitive Partners may wish to consider using Special Delivery or a contracted courier under tracked conditions;
 - If information is to be sent via fax, then safe haven procedures must be used;
 - Information sent in hard copy must be addressed to a specific person and marked '*for addressee only*'.
- Where datasets (defined as a collection of records, which may be personal data) are exchanged between WEISF members, the format, frequency, intervals and security will be documented, and agreed between the parties involved.

The format and frequency will depend upon the circumstances in which the information is being shared.

Data will be shared regularly as required for the purposes specified. In particular data sharing will support:

- the requirements of the *Essex Safeguarding Children Board* and the *Essex Safeguarding Adults Board* meetings;
- any inspection regimes, timescales and requests; in addition, some anonymised (or pseudonymised) information may only be released at certain points in the year to prevent individuals being identified.

7. Data Retention

Information will be retained in accordance with each partners' data retention policy and in any event no longer than is necessary.

If information is printed from an electronic system, it will be the partner's responsibility to dispose of the information in a secure manner e.g. cross head shredding or incineration, in line with each Partner's policies.

8. Responsibility for exchanging these data and ensuring data are accurate

WEISF members are expected to ensure as far as possible that the information they share and receive is accurate; and to differentiate between observations, allegations, facts and opinions.

WEISF members receiving shared information are responsible for applying relevant quality assurance before using the information.

If information is found to be inaccurate, it is the responsibility of the WEISF member discovering the inaccuracy to notify the appropriate data controller. The data controller will ensure that the source data is corrected and will notify all recipients, who will be responsible for updating the information they hold.

WEISF members will not be liable for any financial or other costs incurred by other parties to this protocol as a result of any information being wrongly disclosed by another party to this protocol or as a result of any negligent act or omission by another party to this protocol.

The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

Everyone sharing data under this agreement is responsible for the quality of the data they are sharing.

Before sharing data, officers will check that the information being shared is accurate and up to date to the best of their knowledge. If sensitive data is being shared which could harm the data subject if it was inaccurate, then particular care must be taken.

If a complaint is received about the accuracy of personal data which affects datasets shared with partners in this agreement, an updated replacement dataset will be communicated to the partners. The partners will replace the out of date data with the revised data.

For the purposes of data shared under this protocol, the Partners are data controllers in common.

9. Complaints

Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.

10. Breach of Confidentiality

In the event of a breach of confidentiality, staff should contact their organisation's Data Protection Officer/Information Governance team/Legal advisers for advice and guidance.

Where a breach is identified as serious, it should be reported to the Information Commissioners Office.

All breaches must be recorded and investigated in conjunction with other Partners where relevant, and in accordance with the regulatory requirements.

11. Agreement

We undertake to implement and adhere to this protocol.

Commencement of the Protocol:

This Protocol shall commence upon date of the signing of a copy of the Protocol by the signatory partners. The relevant information can be shared between signatory partners from the date the Protocol commences.

Withdrawal from the Protocol:

Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the other signatories. The partner must continue to comply with the terms of this Protocol in respect of any information that the partner has obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate secure manner.

Signed by Authorised Person

Print:.....

Signed:.....

On behalf of
(Organisation):.....

Date:.....



Signed by Authorised Person

Print:.....

Signed:.....

On behalf of
(Organisation):.....

Date:.....

Signed by Authorised Person

Print:.....

Signed:.....

On behalf of
(Organisation):.....

Date:.....

Signed by Authorised Person

Print:.....

Signed:.....

On behalf of
(Organisation):.....

Date:.....



Appendix A:

CONFIDENTIALITY AND INFORMATION SHARING

1. THE PERSON

1.1 Expectations

An adult or child with care and support needs is entitled to expect that all information held on them in whatever form is treated with confidentiality.

Personal information should only be shared with the person's agreement (or their parent/Carer/Representative). Where concerns regarding capacity to give this agreement arise, please see 2.2 below.

The person should be aware that information is shared within agencies on a need to know basis.

The person can expect that information is shared in a confidential manner. This applies to sharing within agencies as well as between agencies.

1.2 Consent

If a person has disclosed a potential abuse or a third party has reported a potential abuse, it must be explained that the information cannot be kept a secret between them and the member of staff / volunteer, but must be shared with their agency's management.

The person should also be aware that their circumstances may be referred to Adults or Childrens Social Care even though they may not wish this.

The person can ask that the information is only shared as part of the decision in respect of the safeguarding meeting and the potential abuse is not pursued to investigation.

In this case they must be made aware that this can be overridden in certain circumstances

If this is the case the reasons for this and the procedure must be fully explained to the person and their family / carer. They should be given a chance to reconsider their withdrawal of consent. All this must be fully recorded both as part of the safeguarding meeting.

The person does not want a referral

Issues of capacity and consent must be considered

The wishes of the individual (or their parent/carer) must be respected but the safeguarding meeting needs to consider the wider picture when considering how to proceed. They need to consider some of the following:

- Is it in the public interest to proceed?
- Is there a question of proportionality i.e. does the public duty to protect people override the human rights of the individual?
- Is it lawful to proceed even though the individual does not wish this?
- If an investigation is pursued or abandoned can that decision be justified in terms of the statutory authorities' duty to be accountable?
- Is there a necessity to proceed and override the rights of the individual?

2.1 When consent can be overridden

- A serious crime has been committed
- Where the alleged perpetrator may go on to abuse other adults or children
- Other adults or children are at risk in some way
- The adult or child is deemed to be in serious risk
- There is a statutory requirement e.g. Children's Act 1989, Mental Health Act 1983, Care Standards Act 2000
- The public interest overrides the interest of the individual
- When a member of staff of a statutory service, a private or voluntary service or a volunteer is the person accused of abuse, malpractice or poor professional standards.

2.2 Capacity to consent

If a practitioner considers that an adult may not have the capacity to give 'informed consent' for information sharing, they must follow the [Mental Capacity Act 2005 Code of Practice](#). If you judge that an individual does not have the capacity to make decisions, their views should still be sought as far as possible.

3. INTERAGENCY SHARING OF INFORMATION

3.1 Responsibilities of individual employees

- To record and maintain records in a confidential manner and to share information on a need to know basis.
- To realise information belongs to their agency and not them as an individual. They should never make promises to a person, which they cannot keep, in respect of information sharing.
- To refer to their agencies' own policy on confidentiality and information sharing.



- To ensure confidentiality standards should apply even if the person does not have capacity to give consent to information sharing.

3.2 Responsibilities of agencies

All agencies have a duty to inform Adult or Children Social Services as the lead agency that a potential abuse that has taken place.

If the person has not given consent and the circumstances do not require the overriding of this, Adult or Children Social Care should keep the required information sharing within the safeguarding meeting and for overall monitoring purposes as required in *Care Act*.

If the safeguarding meeting agrees that another agency is the key investigator then only Adult or Children Social Care should retain the information shared at the safeguarding meeting, until such time as the outcome of the investigation is reported back for the safeguarding plan to be put in place, if required.

3.3 Sharing information with the Police

Early discussions with the Police are required if a possible crime has been committed.

This can be on an anonymous basis in the first instance to enable the Police to give advice.

The Police can only proceed if the person has given consent or the circumstances are such that this must be overridden.

Protocols in relation to the Crime and Disorder Act 1998 are also relevant.

3.4 Sharing information from other investigations

There are situations when other investigations will be undertaken as part of the strategy for the enquiry into a potential abuse. The details of those investigations cannot always be fully shared or can only be shared after the investigation is completed.

Discussions can take place between the Police undertaking a criminal investigation and the lead person for the disciplinary proceedings to agree what information / interviews can be shared to assist both processes.

4. PRINCIPLES OF INFORMATION SHARING

4.1 Caldicott

These outline the principles for the sharing of information.

This guidance accepts that information may need to be shared in the best interests of the person concerned, and explains the possible circumstances and the safeguards required.



- All information will only be shared on a 'need to know basis' when it is in the best interests of the person
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained, but if this is not possible and other adults or children are at risk, it may be necessary to override the requirement
- It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other people may be at risk.

4.2 Guiding Principles

Information shared must be only that which is specific to the situation being discussed or information that has a bearing on the situation.

Information should only be shared with those who have a direct interest in the decision making, planning, and service provision or protecting of the adult or child.

The requirements of the Data Protection Act must be observed in relation to information held on the individual.

Good communication between agencies is essential when dealing with situations of potential abuse.

Appendix B: Relevant legal statutes

Care Act 2014
Children Act 2004
Children and Young Persons Act 2008
Crime and Disorder Act 1998
Criminal Justice Act 1967
Common Law Duty of Confidence (Social Services, medical profession, patient confidentiality, Police, Nurses, Health Visitors and Midwives).
Confidentiality – NHS Code of Practice Nov 2003
Domestic Violence Crime and Victims Act 2004
Family Law Act 1996
Fraud Act 2006
Medicines Act 1969
Offences Against the Person Act 1861
Police and Criminal Evidence Act 1970
Protection from Harassment Act 1997
Public Order Act 1986
Sexual Offences Act 1956 / 1967 / 2003
Sex Offenders Act 1997 / 2003
Theft Acts 1968 and 1978
Carers (Recognition and Services) Act 1995
Carers and Disabled Children Act (2000)
Care Standards Act 2000
Chronically Sick and Disabled Persons Act 1970
Community Care (Direct Payments) Act 1996
Disabled Persons (Service Consultation and Representation) Act 1986
Employments Rights Act 1996
Health and Social Care Act 2001/ 2015
Health Service and Public Health Act 1968
Health Act 1999
Housing Act 1985 / 1996 / 2004
Local Authority Social Services Act 1970
Localism Act 2011 / 2013
Mental Capacity Act 2005
Mental Health Act 1983 / 2007
National Assistance Act 1948
National Assistance (Amendment) Act 1951
National Health Service Act 1977
National Health Service and Community Care Act 1990
NHS and Community Care Act 1990
Public Health Act 1936 and Public Health Act 1961
Registered Homes (Amendment) Act 1991
Court of Protection Rules 1994
Counter Terrorism and Security Act 2015



Data Protection Act 1998
Disability Discrimination Acts 1995 & 2005
Enduring Power of Attorney Act 1985
Health & Safety at Work Act, 1974
Human Rights Act 1998
Power of Attorney Act 1971
Public Interest Disclosure Act 1998
Race Relations (Amendment) Act 2000
Regulation of Investigatory Powers Act 2000
Safeguarding Vulnerable Groups Act 2006
Social Security (Claims and Payments) Regulations 1987

Appendix C: Data Protection Act Conditions for Processing

Sharing non-sensitive¹ personal information in accordance with this protocol is likely to be lawful if at least one of the following circumstances exists (Data Protection Act 1998 **schedule 2 conditions**):

- *The data subject has given their consent to the processing.*
- *The processing is **necessary** to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*
- *The processing is **necessary** in order to protect the vital interests of the data subject. In this condition, ‘vital interests’ refers to matters of life or death.*
- *The processing is **necessary** –
for the administration of justice;
for the exercise of any functions conferred by or under any enactment;
for the exercise of any other functions of a public nature exercised in the public interest.*
- *The processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, **except** where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.*

Sharing sensitive² personal information in accordance with this protocol is likely to be lawful if at least one of the following circumstances exists in addition to one of the above (Data Protection Act 1998 **schedule 3 conditions**):

- *The data subject has given his **explicit** consent to the processing of the personal data (See Appendix A).*

*The processing is **necessary** –*

- (a) *in order to protect the vital interests of the data subject or another person, in a case where –*
 - (i) *consent cannot be given by or on behalf of the data subject, or*
 - (ii) *the data controller cannot reasonably be expected to obtain the consent of the data subject, or*

¹ For the purposes of this protocol, sensitive personal information is as defined in the Data Protection Act 1998. All other personal information is deemed to be non-sensitive. Information about physical or mental health is classed as sensitive.

² For the purposes of this protocol, sensitive personal information is as defined in the Data Protection Act 1998. All other personal information is deemed to be non-sensitive. Information about physical or mental health is classed as sensitive.


- (b) *in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.*
- *The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.*
 - The processing –*
 - (a) *is **necessary** for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),*
 - (b) *is **necessary** for the purpose of obtaining legal advice, or*
 - (c) *is otherwise **necessary** for the purposes of establishing, exercising or defending legal rights.*
- *The processing is **necessary** –*
 - (a) *for the administration of justice;*
 - (b) *for the exercise of any functions conferred by or under any enactment; or the processing is **necessary** for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by –*
 - (a) *a health professional (as defined in section 69 of the Act); or*
 - (b) *a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.*
- *The processing –*
 - (a) *is of sensitive personal data consisting of information as to racial or ethnic origin;*
 - (b) *is **necessary** for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and*
 - (c) *is carried out with appropriate safeguards for the rights and freedoms of data subjects.*
- *The processing –*
 - (a) *is in the substantial public interest;*
 - (b) *is necessary for the purposes of the prevention or detection of any unlawful act; and*
 - (c) *must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.*
- *The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.*

Appendix D - Signatories

Organisation Name	ICO	Email
County/District/Borough Councils		
Essex County Council	Z2120726	Informationgovernanceteam@essex.gov.uk
Basildon Borough Council	Z5361180	alex.mclellan@basildon.gov.uk
Braintree District Council	Z5103738	Chero@Braintree.gov.uk
Brentwood Borough Council	Z2092695	Tim.Huggins@brentwood.gov.uk
Castle Point Borough Council	Z588703X	bdelf@castlepoint.gov.uk
Chelmsford City Council	Z7829039	John.breen@chelmsford.gov.uk
Colchester Borough Council	Z5733593	sarah.welham@Colchester.gov.uk
Epping Forest District Council	Z5033101	dnewton@eppingforestdc.gov.uk
Harlow District Council	Z7603332	declan.white@harlow.gov.uk
Maldon District Council	Z6616948	ray.ware@maldon.gov.uk
Rochford District Council	Z6617133	Julie.O'brien@Rochford.gov.uk
Southend Borough Council	Z6029331	IndiraniViknaraja@southend.gov.uk
Tendring District Council	Z577148X	mknappett@tendringdc.gov.uk
Thurrock Council	Z8228055	rsteel@thurrock.gov.uk
Uttlesford District Council	Z5060641	amose@uttlesford.gov.uk
Health		
Anglian Community Enterprise (ACE)		lisa.poynter@acecic.nhs.uk
Basildon and Brentwood CCG	ZA007615	jane.marley@nhs.net
Basildon and Thurrock University Hospitals NHS Foundation Trust	Z6288182	matthew.barker@btuh.nhs.uk
Castle Point and Rochford CCG	ZA007607	c/o jane.marley@nhs.net
Colchester Hospital University Foundation Trust	Z6601302	Barry.Moult@colchesterhospital.nhs.uk
East of England Ambulance NHS	Z955129X	Emma.Sears@eastamb.nhs.uk
Hertfordshire Partnership Foundation Trust	Z1377585	
Mid Essex CCG	ZA007619	c/o jane.marley@nhs.net
Mid Essex Hospital Services NHS	Z9751505	Bhaves.Khetia@meht.nhs.uk
North East Essex CCG	ZA007604	c/o jane.marley@nhs.net
North East London Foundation Trust	Z9096541	Robert.Paley@nelft.nhs.uk
North Essex Partnership Trust	Z5405315	c/o alice.williams@sept.nhs.uk
One to One (North West) Limited	Z235894X	katie@121midwives.co.uk
Princess Alexandra Hospital NHS	Z8759485	Tracy.Goodacre@pah.nhs.uk
South Essex Partnership Trust	Z5344366	alice.williams@sept.nhs.uk
Southend CCG	ZA008459	c/o jane.marley@nhs.net
Southend University Hospital NHS	Z1972899	Tracey.Kalp@southend.nhs.uk
Thurrock CCG		c/o jane.marley@nhs.net
Virgin Care Limited	Z9796937	Sarah.Murray@virgincare.co.uk
West Essex CCG	ZA015050	c/o jane.marley@nhs.net
Justice		
Community Rehabilitation Company	ZA058886	
Essex Police	Z4883472	Andy.begent@essex.pnn.police.uk

HMP Chelmsford		Lee-ann.williams@hmpps.gsi.gov.uk Tony.miller@hmpps.gsi.gov.uk
National Probation Service (Essex)		
Voluntary and Community Sector		
Barnardo's	Z5951768	pat.greene@barnardos.org.uk veronika.neyer@barnardos.org.uk
Changing Pathways (formerly Basildon Women's Aid)	Z6636508	Welcome@changingpathways.org Sue.Davis@changingpathways.org
The Children's Society	Z9480097	Kerry.Horner@childrenssociety.org.uk
Colchester & Tendring Women's Refuge	Z5395485	
Essex Change	ZA154272	Lora.Draper@relate-northersex.org
Independent Living Advocacy	Z5366828	
Provide		Stephen.Woodford@nhs.net
Respect	ZA059045	Neil.Blacklock@respect.uk.net
Safelives	Z2719216	Sonal.Shenai@safelives.org.uk
Safer Places	Z6584606	allison.gardner@saferplaces.co.uk
Thurrock Women's Aid (??)	Z7141773	
Housing		
CHP	Z7619300	terri.cochrane@chp.org.uk
Colchester Borough Homes	Z8259492	info@cbhomes.org.uk
Colne Housing	Z5625710	
Estuary Housing	Z5301256	Natalie.schofield@estuary.co.uk
Family Mosaic	Z8389531	
Greenfields	Z1122456	jenny.upton@GreenfieldsCH.org.uk
London and Quadrant (L&Q)		
Moat Housing		Tracy.kinton@moat.co.uk
One Support		
South Essex Homes	Z9210005	sehcustomerservices@seh.southend.gov
Sanctuary Housing / Rochford		contactus@sanctuary-housing.co.uk
Essex Fire & Rescue Service		Tracy.King@essex-fire.gov.uk

Appendix E – Standard Operating Procedures

MARAT Operating Procedures	 DRAFT Essex MARAT operating protocol v1