INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Overarching Safeguarding across geographic Essex

All agencies involved in safeguarding activities across geographical Essex are partners to this protocol, and partners relevant to each programme of work are named in the relevant Sharing Specific for Programme in the appendices

Version Control	
Date Agreement comes into force	June 2019
Date of Agreement review	June 2022
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Gemma Gibbs
Status of document – DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	V1

Wider Eastern Information Stakeholder Forum

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 Agency
Privacy Impact Assessment (PIA/DPIA)		
Supporting Sharing Specific for Programme		WEISF holds copies of SSPs
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the WEISF Portal.

1.	Purpose	REFERENCES

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.

GDPR
Go to article 5

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, Southend and Thurrock **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 of an offender.

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

Each specific programme or project will have a Sharing Specific for Programme (SSP) in place to define the detail of what is shared, with whom and how. Please see appendices where the SSPs are held.

GDPR
Go to articles 6 - 9

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 Sharing Specific for Programme in the appendices.

- 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 an 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 the risk posed by people who are convicted of offences against children and vulnerable adults and who are potential offenders;
- Information required to manage risks and formulate safety plans for victims and their families in Essex, Thurrock and Southend via the Local Safeguarding Children Board and the Safeguarding Adults Board meetings;
- Information required for safeguarding reviews such as Learning Reviews (formerly known as Serious Case Reviews), Safeguarding 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

General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.

GDPR

Go to articles 6-14

Personal Data (identifiable data)	**Special Categories of Data (Sensitive identifiable data)**
Article 6:	Article 9: (if appropriate):
Legal Obligation	Vital Interests
Public Task	Substantial Public Interest
Vital Interests	Health & Social Care

Other legislation or statute as follows

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 Public Health Act 1936 and Public Health Act 1961 Public Health Act 1936 and Public Health Act 1961	NHS and Community Care Act 1990 Registered Homes (Amendment) Act 1991 Registered Homes (Amendment) Act 1991
Court of Protection Rules 1994	Counter Terrorism and Security Act 2015
Data Protection Act 2018	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	Serious Crime Act 2015
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)	

<u>The Caldicott principles</u>

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.

Other legislation and guidance

- 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.

4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

For the purposes of this Protocol the responsibilities are defined as follows: For help go to https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN Articles 24 – 29 where these roles are explained.	Tick box	Organisation Name(s)
The Sole Data Controller for this sharing is:	☐	
The Joint Data Controllers for this sharing are:	☒	All Signatories
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Refer to the Sharing specific for Programme in Appendices
Data Processors party to this protocol are (please list):	☐	

This Protocol will be reviewed three years after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by Essex County Council. New initiatives will be covered by Sharing Specific for Programme agreed by the relevant Partners and this protocol will be republished with each addition.

5. Subject Rights

Essex Partner Agencies' Information Sharing Agreements are made publicly available on the Whole Essex Information Sharing Framework website to enable compliance with article 12 of the GDPR.

It is each Partner's responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	Processes are in place to enact this right - please check the box
GDPR Article 13&14 – **Right to be Informed** – Individuals must be informed about how their data is being used. This sharing must be reflected in your privacy notices to ensure transparency.	☒
GDPR Article 15 – **Right of Access** – Individuals have the right to request access to the information about them held by each Partner	☒
GDPR Article 16 – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	☒
GDPR Article 17 (1)(b)&(e) – **Right to be forgotten** – This right may apply where the sharing is based on Consent, Contract or Legitimate Interests, or where a Court Order has demanded that the information for an individual must no longer be processed. Should either circumstance occur, the receiving Partner must notify all Data Controllers party to this protocol, providing sufficient information for the individual to be identified, and explaining the basis for the application, to enable all Partners to take the appropriate action.	☐
GDPR Article 18 – **Right to Restriction** – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☐

GDPR
Go to articles 12 – 15

GDPR

GDPR Article 19 – **Notification** – Data Controllers must notify the data subjects and other recipients of the personal data under the terms of this protocol of any rectification or restrict, unless it involves disproportionate effort.	☒	Go to article 16 & 22
Article 21 – **The Right to Object** – Individuals have the right to object to any processing which relies on Consent, Legitimate Interests, or Public Task as its legal basis for processing. This right does not apply where processing is required by law (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☒ **Only where relying on Public task**	
Article 22 – **Automated Decision Making including Profiling** – the Individual has the right to request that a human being makes a decision rather than a computer, unless it is required by law.	☐	
Freedom of Information (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 relates to data requested from a Public Authority by a member of the public. 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 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.	☒	

6. Security of Information

Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
Paper information is stored securely	☒	
Paper and electronic information is securely destroyed with destruction log for electronic information	☒	
Laptops and removable media such as memory sticks are secured when not in use	☒	
Technical security appropriate to the type of information being processed is applied	☒	
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	☒	
Disaster recovery arrangements are in place	☒	
Encryption of personal data is fully implemented	☒	
Data minimisation has been considered	☒	
Can pseudonymised or anonymised data be used to meet your processing needs?	☐	
There are sufficient access controls for systems/networks in place	☒	

Routine and regular penetration tests are carried out	☒
Article 40 Codes of Conduct are adhered to (where applicable)	☐
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	☒
Confirm entry in Records of Processing Activity	☒
Additional measure 1 – please specify here	☐
Additional measure 2 – please specify here	☐

Partners receiving information will:

- Ensure that their employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
- Protect the physical 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 an up to date policy for handling personal data which is available to all staff
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

International Transfers (Where applicable)

If any personal data is to be transferred outside of the EEA, please ensure you capture the relevant supporting adequacy decision for such a transfer here (articles 40-43).

Adequacy Decision in place https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en	Date of approval by EU Commission is:	[Provide hyperlink here]
ICO Approved standard contract clauses in place https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf	Date of approval by ICO is:	[Provide hyperlink here]

ICO Approved Binding Corporate Rules in place https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/	Date of approval by ICO is:	[Provide hyperlink here]
The Individuals have given explicit consent to the transfer and understand the risks associated with the transfer	Confirm this consent has been recorded appropriately	√ / ×
The receiving organisation in a 3rd country is bound by an approved Code of Conduct recognised by the EU	Date of approval by ICO is:	[Provide hyperlink here]

ICO guidance on International Transfers can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

7. Format and Frequency

See Sharing Specific for Programme in Appendices (These will be published once multi-agency groups have sent them to weisf@essex.gov.uk)

8. Data Retention

Information will be retained in accordance with each partners' published data retention policy available on their websites, and in any event no longer than is necessary.

GDPR
Go to article 5

9. Data Accuracy

Please check this box to confirm that your organisation has processes in place to ensure that data is regularly checked for accuracy, and any anomalies are resolved ☒

GDPR
Go to articles 5, 16 - 18

10. Breach Notification

Where a security breach linked to the sharing of data under this protocol is likely to adversely affect an Individual, all involved Partners must be informed within 48 hours of the breach being detected. Please see Sharing Specific for Programme in Appendices for contact information for Partners. The decision to notify the ICO can only be made after consultation with any other affected Partner to this protocol, and notification to the ICO must be made within 72 hours

GDPR
Go to articles 33, 34, 77 - 84

of the breach being detected. Where agreement to notify cannot be reached within this timeframe, the final decision will rest with the Protocol owner as depicted on page 1 of this document. All involved Partners should consult on the need to inform the Individual, so that all risks are fully considered and agreement is reached as to when, how and by whom such contact should be made. Where agreement to notify cannot be reached, the final decision will rest with the Protocol owner as depicted on page 1 of this document. All Partners to this protocol must ensure that robust policy and procedures are in place to manage security incidents, including the need to consult Partners where the breach directly relates to information shared under this protocol.		
11.	**Complaints**	
Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.		GDPR Go to articles 16 – 22 & 77
12.	**Commencement of 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.		
13.	**Withdrawal from the Protocol**	
Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the WEISF administration team weisf@essex.gov.uk. The WEISF administration team will notify other Partners to the Protocol. 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.		
14.	**Agreement**	

This Protocol must be approved by the responsible person within the organisation (SIRO/Caldicott Guardian/Chief Information Officer).

For details of signatories of the Overarching Safeguarding ISP please contact weisf@essex.gov.uk who maintain the approvals list.

15.	SSPs

SSPs are not published on the WEISF Portal. If you need to see a copy please send your request to weisf@essex.gov.uk.