INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Essex Emergency and Major Incident ISP

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, Essex, CM1 1QH	03457 430430	informationgovernanceteam@essex.gov.uk	Paul Turner	**Z6034810**
Essex Police	PO Box 2 Springfield Chelmsford Essex CM2 6DA				**Z4883472**
Essex Fire & Rescue	Service Headquarters London Road Rivenhall Witham Essex CM8 3HB			Hope Osayande	**Z5349761**
Essex Local Authorities (District/Borough/City Councils) –			See appendix A		

Version Control	
Date Agreement comes into force	September 2019
Date of Agreement review	September 2022
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Gemma Gibbs
Status of document – DRAFT/FOR APPROVAL/APPROVED	FINAL
Version	1.0

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 (PIA/DPIA)	PIA 712 – Resilience Direct	Essex County Council
Supporting Standard Operating Procedure		
Associated contract	Kenyon International Emergency Services Contract (Disaster Recovery Services	Essex County Council
Associated Policy Documents		
Other associated supporting documentation		

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

1.	Purpose	REFERENCES
Sharing information between partner organisations in an emergency is vital to the provision of coordinated and seamless humanitarian assistance services to support people affected[1]. However, there are a vast range of situations that would fall outside of the scope of humanitarian assistance but would be an emergency situation or major incident that would require the sharing of information. Eg the identification of vulnerable people that may require specialist assistance during an evacuation or specialist support within their own homes if instructed to stay indoors. These services include activities aimed at addressing the needs of people affected by emergencies: the provision of psychological and social aftercare and support in the short, medium and long term. The types of emergency which may require these services include (but are not limited to); large industrial accidents, aviation incidents, widespread flooding and terrorist attacks. The sharing of information can help to meet the requirements of statutory legislation, government guidance and local initiatives. This Information Sharing Protocol (ISP) sets out the overarching information principles between those listed in Appendix A (hereinafter known as the "partner organisations") in sharing data in the event of an emergency or major incident. This ISP aims to: • Avoid duplication of effort • Assist in the provision of appropriate and timely assistance to people affected in the short, medium and longer term • Ensure a seamless approach to the provision of assistance between partner organisations • Collate information to enable the identification and prioritisation of those in need of assistance • Assist in decision making and prioritising resources to assist those most in need Information may only be shared for the purposes above. This protocol is linked to the following plans and protocols (and associated plans which exist beneath these, such as plans for activating options from the Humanitarian Assistance Plan Toolkit, e.g. Crisis Support Team for Essex Protocols, Essex Resilience Forum (ERF) Humanitarian Assistance Centre Plan): • ERF Combined Operating Procedures for Essex • ERF Humanitarian Assistance Plan • ERF Recovery Guide • Vulnerable Persons and Premises Identification Protocol • ERF Evacuation Plan	GDPR Go to article 5

[1] Those affected can include: survivors, family/friends of those missing, killed or survivors, witnesses and the affected community.

Definitions for the purpose of this ISP
Definition of emergency = An event or situation which threatens serious damage to human welfare in a place in the UK, the environment of a place in the UK, or the security of the UK or of a place in the UK.

Definition of major incident = An event or situation with a range of serious consequences which requires special arrangements to be implemented by one or more emergency responder agency.

2. Information to be shared

GDPR
Go to articles 6 - 9

The information to be shared is set out in the table below. The table describes the type of information that may be required to be shared by partner organisations in the event of an emergency or major incident.
"*The starting point for emergency responders should be to consider the risks and potential harm that may arise if they do* ***not*** *share information. However, they should always consider whether the objective could still be achieved by sharing less, or no, personal data.*"
HM Government, Human Aspects Guidance 2016, page 5
Any requests for information from people affected should include a statement that their details may be shared with other organisations and to obtain consent, where possible or reasonably practical.
The information to be shared could consist of (but not limited to):

No	Type of Information	Reason
1	Number of people affected	• Help partner organisations prioritise information • Help partner organisations inform decisions about response/recovery • Aid/inform strategic decision making when undergoing the Humanitarian Impact Assessment • Inform Health Services (Acute Trusts, Mental Health, GPs, Social Care) of potential demands on their services in their area
2	Names, addresses, email addresses and contact numbers and primary language of people affected	• To contact people affected in the future offering support services e.g. Humanitarian Assistance Centre • Direct resources to a particular area in Essex e.g. location of Humanitarian Assistance Centre • Be able to compare information with others to form a complete list of people affected and avoid duplication (e.g. info received from other agencies such as Police)

		• Help deploy Operational Teams[2] • To inform the emergency services during an evacuation.
3	Condition/injuries of survivors (including medication/long term care issues & psychological impacts) and involvement with emergency (i.e. how affected)	• Identify suitable Operational Teams for deployment • Prepare Operational Teams for deployment • Inform Health Services (Acute Trusts, Mental Health, GPs, Social Care) of potential demands on their services in their area
4	Any information that would highlight health and safety issues (e.g. any issues known about individuals which may pose a risk, either to that individual or others)	• Help inform risk assessment (e.g. information about previous convictions may determine if/how many Team Members deploy to assist someone in their own home)
5	Sensitive information e.g. date of birth, faith, gender	• Help identify suitable Operational Teams for deployment • Help prepare Operational Teams for deployment • Avoid duplication and causing distress
6	Next of Kin	• To contact next of kin offering support • To assist people contacting their next of kin should they wish to do so
7	Casualty Bureau categorisation groups information (including names, addresses and contact information)	• Prioritising and filtering support services • Informing non-Essex residents of available support services
8	Name, address, date of birth, gender, details of known vulnerabilities	• The identification of vulnerable people during or in the recovery to an emergency. • Examples: Informing evacuation plans, supporting people in their own homes following an emergency.

3. Legal Basis

[2] Operational Teams can include: Crisis Support Workers, Incident Care Team Members, British Red Cross Workers, Health Workers, Faith Representatives and Social Care Teams

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

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

The Civil Contingencies Act 2004 places a duty upon organisations, including Local Authorities to share information and co-operate.
"*Category 1 and 2 responders are obliged to co-operate with other Category 1 and 2 responders and other organisations engaged in response in the same local resilience area*" HM Government, Emergency Preparedness, page 10.
"*Under the Civil Contingencies Act, Category 1 and 2 responders have a duty to share information with other Category 1 and 2 responders. Information sharing is also encouraged as being good practice*"
HM Government, Emergency Preparedness, page 24.

It is generally good practice to seek the consent of individuals to share their information. However disclosure may be lawful in certain circumstances without consent, for example the performance of public functions, legal obligations, prevention/detection of crime.
"*Consent is only one of a number of conditions under which personal data can be shared. In an emergency situation, or in the aftermath, personal data can be shared if responders consider it is necessary to protect the individual where there is a risk of significant harm to life, or for example, if it forms part of the exercise of functions in the public interest (i.e. activities to address the HA [Human Aspects] arising from an emergency).*"
HM Government, Human Aspects Guidance, page 5-6

GDPR
Go to articles 6-14

Other legislation or statute as follows:

- Civil Contingencies Act 2004
- Localism Act 2011
- Care Act 2014
- Health and Social Care Act 2012
- Children Act 2004
- Housing Act 1996
- Human Rights Act 1998
- HM Government 2007 Data Protection and Sharing – Guidance for Emergency Planners and Responders
- NHS Patient Confidentiality

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.
All partner organisations are responsible for publishing their own privacy notices. These notices should state what information is being collected, for what purpose and who it might be shared with.
In an Emergency Assistance Centre[3] where information is collected, notices should be displayed providing details to the public about where they can view more detailed privacy notices.
Where forms are used to collect information, they should contain a statement linking with the privacy notices.

Fair processing requirements have been satisfied by the Privacy Notice of all signed partners.

Essex County Council's privacy notice can be viewed here.

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 partners listed on the Summary Sheet (Page 1)

[3] Emergency Assistance Centres include: Survivor Reception Centres, Family & Friends Reception Centres, Rest Centres and Humanitarian/Community Assistance Centres.

In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Essex County Council	
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 Civil Protection & Emergency Management, Essex County Council.

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.

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 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.	☒	GDPR 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.	☒	
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	Date of approval by ICO is:	[Provide hyperlink here]

https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/		
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

The format the information will be shared will be dependent on the emergency situation and facilities available at that time.
The method(s) by which information will be shared will be in any of the following, with consideration to the appropriate technical security for information transfer:

- Resilience Direct which is the Government provided information sharing platform (see PIA ref 712 held by Essex County Council's Information Governance Team)
- Secure email (eg. PSN including GCSX, PNN and nhs.net / Egress / Password Protected document)
- Hard copy of paper file
- Telephone communication
- Fax machine using Safe Haven Procedures

The frequency with which the information will be shared is on an adhoc basis as required for the purposes specified.

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

GDPR

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 ☒		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. The email addresses on page 1 should be used to contact the 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 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.		GDPR Go to articles 33, 34, 77 - 84
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).

Approver Name	
Organisation Name	
Date of Agreement	

Please submit this Protocol to weisf@essex.gov.uk with list of approved signatories. The Protocol will then be published on weisf.essex.gov.uk.

Email approvals will only be accepted from an authorised signatory role from each organisation. Please see the list of authorised roles per organisation on WEISF.essex.gov.uk

15. APPENDICES

Appendix A – List of Essex Local Authorities

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Southend Borough Council	Civic Centre Victoria Avenue Southend on Sea Essex SS2 6ER	01702 215000	council@southend.gov.uk		**Z6929331**
Thurrock Council	PO Box 1 Civic Offices New Road Grays Thurrock Essex RM17 6SL				**Z8228055**
Chelmsford City Council	Civic Centre Duke Street Chelmsford Essex CM1 1JE				**Z7829039**
Harlow District Council	Civic Centre The Water Gardens College Square Harlow Essex CM20 1WG				**Z7603332**
Epping Forest District Council	Civic Offices High Street Epping Essex CM16 4BZ				**Z5033101**
Brentwood Borough Council	Town Hall Ingrave Road Brentwood				**Z2092695**

	Essex CM15 8AY				
Basildon Borough Council	The Basildon Centre St Martins Square Basildon Essex SS14 1DL				**Z5361180**
Castle Point Borough Council	Council Offices Kiln Road Benfleet Essex SS7 1TF				**Z588703X**
Rochford District Council	Council Offices South Street Rochford Essex SS4 1BW				**Z6617133**
Maldon District Council	Princes Road Maldon Essex CM9 5DL				**Z6616948**
Uttlesford District Council	London Road Saffron Walden Essex CB11 4ER				**Z5060641**
Braintree District Council	Causeway House Bocking End Braintree Essex CM7 9HB				**Z5103738**
Colchester Borough Council	33 Sheepen Road Colchester Essex CO3 3WG				**Z5733593**
Tendring District Council	Town Hall Station Road Clacton On Sea				**Z577148X**

	Essex CO15 1SE				