Information Sharing Protocol / Data Sharing Agreement

SUMMARY SHEET

Title of Agreement: Emergency Planning 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	034570 430430	dpo@essex.gov.uk	Paul Turner	Z6034810
Essex Police	PO Box 2. Springfield. Chelmsford. CM2 6DA	01245 491491	DPO@essex.police.uk	Michelle Watson	Z4883472
Essex Fire & Rescue	Service HQ London Road Rivenhall. Witham CM8 3HB	01376 576000	informationgovernanceteam@essex-fire.gov.uk	Lauri Almond	Z5349761
Essex Local Authorities & other multi-agency partners			**See Appendix B**		

Version Control

Date Protocol comes into force	August 2024
Date of next Protocol review	August 2027
Protocol Lead Organisation	Essex County Council
Protocol drawn up by (Author(s))	Gemma Gibbs, Senior Information Governance Officer
Status– DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	3.0

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. We recommend that these protocols are published alongside your online privacy notices for full transparency.

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:

- 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**
Data Protection Impact Assessment (DPIA)	ResilienceDirect TM	HM Government Cabinet Office
Supporting Standard Operating Procedure		
Associated contract	Kenyon International Emergency Services Contract (Disaster Recovery Services	Essex County Council
Associated Policy Documents		
Other associated supporting documentation	Identifying and supporting persons who are vulnerable in an emergency. Supporting guidance for Local Resilience Forums in England (March 2024) Data Protection and Sharing in Emergencies – 2 page summary for Cat 1 and 2 responders	HM Government

	Data Protection and Sharing – Guidance for Emergency Planners and Responders Ministry of Justice – legal advice and jargon buster Emergency Preparedness document	

1 – Purpose

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. Example: *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 emergencies 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 Response and Recovery Framework
- ERF Humanitarian Assistance Plan
- ERF Recovery Framework
- ERF Vulnerable Persons and Premises Identification Protocol

- ERF Evacuation Plan

Under the Civil Contingencies Act 2004 (CC Act), Category 1 and 2 responders have a duty to share information with other Category 1 and 2 responders. This is fundamental to their ability to fulfil the range of other civil protection duties under the act, including emergency planning, risk assessment and business continuity management. The statutory guidance on the CC Act also encourages information sharing between responders. In most instances, information will pass freely between Category 1 and 2 responders, as part of a more general process of dialogue and co-operation. But there are still some instances in which the supply of information will be more controlled, and hence a formal request for information may be appropriate.

Not all information can be shared, and the CC Act allows exceptions from the supply of some sensitive information. There are broadly 4 kinds of sensitive information:

1. Information prejudicial to national security
2. Information prejudicial to public safety
3. Commercially sensitive information
4. Personal information

Of course, there are different degrees of sensitive information. The guidance to accompany the Act, Emergency Preparedness, clearly states that some sensitive information may be suitable for some audiences but not others. The Act also offers safeguards that make clear that sensitive information can still be shared between Category 1 and 2 responders for emergency planning purposes – the organisation providing the information can specify that the information may only be used for the purpose for which it was requested.

Planning for vulnerable persons

Category 1 responders (with the cooperation of Category 2 responders) have responsibilities to plan for and meet the needs of those who may be vulnerable in emergencies. For more information refer to the Identifying and supporting persons who are vulnerable in an emergency.pdf published by HM Government.

Reference material

Emergency Preparedness (2011) Chapter 5 Emergency Planning; paragraphs 5.97 to 5.103 detail 'the vulnerable' as 'people who are less able to help themselves in the circumstances of an emergency'. Cabinet Office
Emergency Preparedness (2012) Chapter 7 Communicating with the Public; paragraphs 7.72 to 7.77: reaching vulnerable persons. Cabinet Office Emergency Preparedness (2012) Chapter 8 Business continuity advice. Cabinet Office

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 a 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.

In line with Emergency Preparedness statutory guidance[1] this ISP considers **vulnerable** to mean:
'*People who are less able to help themselves in the circumstances of an emergency, who must be given special consideration in plans.'*

ResilienceDirect™- Resilient communications - GOV.UK (www.gov.uk)

ResilienceDirect™ provides a secure web service for category 1 and 2 emergency planners and responders to host and share information. This is an auditable service, from which emergency planners and responders can monitor and review access to data. To support multi-agency sharing of information, emergency practitioners should use ResilienceDirect™ to work together – across geographical and organisational boundaries – during the preparation, response and recovery phases of an event or emergency. The service enables organisations to undertake planning and exercising for and managing live incidents leading to enhanced multi-agency working practices, ensuring that information is readily and consistently available to users. Group Administrators editors responsible for managing their organisational group membership and pages.

Essex Resilience Forum – partner organisations
A number of agencies and organisations come together in partnership to create the ERF. The Civil Contingencies Act gives a category to the different agencies and organisations that belong to the Forum; those involved in responding are defined as Category 1 Responders and those who may be called upon to provide essential support or advice during an incident are Category 2 Responders. A list of partners is provided below:

Category 1 Responders

- British Transport Police
- East of England Ambulance Service
- Essex County Council
- Essex County Fire & Rescue
- Essex Police
- Environment Agency
- Maritime & Coastguard Agency

- Met Office
- NHS England (Essex Area)
- NHS Hertfordshire & West Essex ICB
- NHS Mid & South Essex ICB
- NHS Suffolk & North Essex ICB
- Port Health Authority
- UK Health Security Agency
- Basildon Borough Council
- Braintree District Council
- Brentwood Borough Council
- Castle Point Borough Council
- Chelmsford City Council
- Colchester Borough Council
- Epping Forest District Council
- Harlow Council
- Maldon District Council
- Rochford District Council
- Southend on Sea City Council
- Tendring District Council
- Thurrock Council
- Uttlesford District Council

Category 2 Responders

- Abellio Greater Anglia
- Affinity Water
- Anglian Water
- c2c
- Cadent Gas Networks
- Essex & Suffolk Water

- Harwich Haven Authority
- Harwich International Port
- Highways Agency
- London Overground Trains
- London Southend Airport
- London Stansted Airport
- National Grid Plc
- Network Rail
- Openreach
- Port of London Authority
- Port of Tilbury
- Telecommunications Providers
- Transport for London / Underground
- UK Power Networks

The ERF has developed the Essex Emergency Voluntary Network (EEVN) to ensure that relationships are built with the voluntary sector to help work together during incidents. The voluntary community have access to a wide range of skills and expertise which can be invaluable when dealing with an emergency.

Some scenarios where the voluntary sector can assist are:

- The search for missing vulnerable or confused people
- Humanitarian Assistance
- Prescription collection and delivery
- Transport of resources & personnel during adverse weather or flooding
- Wide area communications and door knocking

Essex Voluntary Sector Partners

- 4x4 Response UK (Essex)
- Ascension Trust Response Partners
- British Red Cross

- Council for Voluntary Services / Volunteer Essex
- Crisis Support Team Essex (now a part of Essex County Council)
- Essex Search & Rescue
- Joint Civil Aid Corps
- RAYNET UK
- RNLI Lifeboats
- Royal Voluntary Service
- RSPCA
- Salvation Army
- Samaritans
- Scouts (Essex)
- St John Ambulance

1 Emergency Preparedness**. Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements. Chapter 5, Paragraph 5.99, 'The vulnerable'. Cabinet Office.**

2 – Information to be shared

The information to be shared is set out 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

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 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 Operation Teams (can include: Crisis Support Workers, Incident Care Team Members, British Red Cross Workers, Health Workers, Faith Representatives and Social Care Teams).
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 and gender	• Help identify suitable Operation 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

The identified conditions for processing under the Data Protection Act 2018:

Partner to Protocol	Personal Data (identifiable data)	Special Categories of Data (Sensitive identifiable data – if applicable)	Law Enforcement data (if applicable e.g. community safety)
Organisation Name(s)	**Article 6:**	**Article 9: (if appropriate):**	**DPA Part 3 (if appropriate):**
Public Body Category 1 & 2 Responders –	**Vital Interests**	**Vital Interests**	**Substantial Public Interest**
	Public Task	**Substantial Public Interest**	**Vital Interests**
	Legal Obligation	**Public Interest in Public Health**	
Non-Public Body Category 2 Responders –	**Legal Obligation**	**Substantial Public Interest**	**Substantial Public Interest**
	Public Task		
Voluntary Sector	**Public Task**	**Health & Social Care**	
	Consent	**Explicit Consent**	
	Legal Obligation	**Public Interest in Public Health**	

Where the data sharing involves Special Category Personal Data or Law Enforcement Data all Partners to the protocol confirm they have an Appropriate Policy Document in place ☒

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

Please list below relevant legislation or statute empowering this sharing activity: Legislation guides | Local Government Association

Civil Contingencies Act 2004
Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 – Part 8 (Information), Sections 45 to 54
HM Government – Identifying and supporting persons who are vulnerable in an emergency. Supporting guidance for Local Resilience Forums in England 2024 (Reason for amendment, review of 2008 guidance).
Equality Act 2010
Public Sector Equality Duty (PSED) contained in the Equality Act 2010
Localism Act 2011
Local Government Act 2000
Care Act 2014
Children Act 2004
Children and Social Work Act 2017
Education Act 2002
The Child Safeguarding Practice Review and Relevant Agency (England) Regulations 2018
Emergency planning and response for education, childcare and children's social care settings (2023), Department for Education
NHS Emergency Preparedness, Resilience and Response Framework (2022), NHS England
Health and Care Act 2012/2022
Housing Act 1996
Human Rights Act 1998

HM Government 2007 Data Protection and Sharing – Guidance for Emergency Planners and Responders
NHS Patient Confidentiality
The National Health Service Act 2006
Security and Emergency Measures Direction (2022) (section 4.4.d)
Emergency Planning Guidance, DEFRA
General Conditions of Entitlement, Ofcom
Protecting access to emergency organisations when there is a power cut at the customer's premises (2018), Ofcom
Radiation (Emergency Preparedness and Public Information) Regulations 2019 (REPPIR), the Approved Code of Practice, Office for Nuclear Regulation
Emergency Preparedness (2011) Chapter 14 The role of the voluntary sector, Cabinet Office
Planning the coordination of spontaneous volunteers (2019), Cabinet Office
Vulnerable children and young people, and critical workers (2023) Department for Education
Evacuation and Shelter (2014) Non-statutory guidance to complement Emergency Preparedness and Emergency Response (Cabinet Office)

4. Responsibilities

For help go to Controllers and processors | ICO

DATA CONTROLLERS - Organisation Name(s)	Data Protection Status	Provide Data	Access Data
All parties to this data protocol	**Controller**	☒	☒

In the event of Joint Controllers, the single point of contact for the sharing will be the lead organisation for the specific emergency or major incident.

DATA PROCESSORS – Organisation Name(s)	Name(s) of Controller managing the Contract or other agreement	DPIA completed
ResilientDirect™ (System being used by partners)	HM Government, Cabinet Office	**Yes**

This Protocol will be reviewed three years after it comes into operation, or sooner should a breach occur or circumstances change, to ensure that it remains fit for purpose. The review will be initiated by the Lead Organisation (see page one).

5. Data Subject Rights

All data controllers are responsible for responding to requests to exercise data subject rights received by their organisation.

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. Partners will respond within one month of receipt of a notice to exercise a data subject right. Each Partner has a legal responsibility to ensure they have appropriate processes in place to support the exercising of these rights by Data Subjects.

It should be noted that where the legal condition for processing under this protocol differs for participating organisations, the applicable rights may also vary. It is for each controller to understand which rights apply in respect of the processing condition they rely on.

Fair processing in accordance with UK 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 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.

Data Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	**Check box to confirm processes are in place**
UK 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. Partners are encouraged to publish their sharing protocols alongside their privac**y** notices to support greater transparency.	☒
UK GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner.	☒

UK GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed**.**	☒
UK 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.	☒
UK GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☒
UK 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 restriction, unless it involves disproportionate effort.	☒
UK GDPR 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. Individuals always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☒
UK GDPR 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. The individual also has the right to object to profiling which places legal effects on them.	**N/A**
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 public authority that received the request. **See Appendix A for more details.**	☒

6. Security of Information

The Partners to this protocol agree that they will apply appropriate technical and organisational security measures which align to the volume and sensitivity of the personal data being processed in accordance with article 32 of the UK GDPR as applied by the Data Protection Act 2018.

The security of the personal data in transit will be assured by:

The security of the personal data in transit will be assured by using the following methods depending on the emergency situation and facilities available at the time:

- Resilience Direct, which is the Government provided information sharing platform.
- Secure email
- Hard copy paper file
- Telephone communication
- Fax machine using Safe Haven procedures

Partners receiving information will:

- Complete a Data Protection Impact Assessment (DPIA) where necessary
- 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 data breaches involving personal data, including notifying relevant third parties of any breach
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

7. International Transfers

No data will routinely be transferred outside the UK. However, if this were required in an emergency situation partners must document the sharing which might legitimately take place either where an adequacy decision is in place or under article 49 (d). You may rely on your need to share data to (exception 6) protect a person's vital interests or (exception 4) for important reasons of public interest.

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/

8. Format & Frequency

- The format the information will be shared in will be dependent on the emergency situation and facilities available at the time.
- The frequency with which the information will be shared is dependent on when an emergency situation arises.

If a shared system is being used by partners:

- What system is being shared? Resilience Direct
- Who is the owner of the system? UK Government
- A DPIA has been completed and approved for the use of this system by the UK Government.

9. 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 for the purpose of this protocol. All data beyond its retention will be destroyed securely.

10. 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 ☒

11. Personal Data Breach Notifications

Where a data 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 all other affected Partners to this protocol, and where notification to the ICO is required, it 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 Lead Organisation as depicted on page one.

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 Lead Organisation as depicted on page one.

All Partners to this protocol must ensure that robust policy and procedures are in place to manage data breaches, including the need to consult Partners where the breach directly relates to information shared under this protocol.

12. Complaint Handling

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

13. 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.

14. Withdrawal from the Protocol

Any partner may withdraw from this protocol upon giving 4 weeks written notice to the Protocol Lead Organisation stated on page one, who will inform other partners to the protocol. The leaving 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.

15. Agreement

This Protocol must be approved by the responsible person within each organisation (DPO/SIRO/Caldicott Guardian/Chief Information Officer). Signed copies should be retained by the Lead Organisation for the lifetime of the Protocol plus two years.

Signed Protocols, or emails of approval should be sent to the Lead Organisation at: DPO@essex.gov.uk

Appendix A - ERF FOIA/EIR Process/ Information Governance Agreement

The Essex Resilience Forum Secretariat, on behalf of ERF partners hold various multi-agency documents that include:

- Risk Assessments
- Emergency Response Plans
- Exercise & Training Materials
- Incident Debriefs
- Meetings & Projects

Whilst the ERF holds copies of a range of multi-agency documents, it owns very few of these, with the vast majority being allocated to one of the forum partners.

MHCLG FOIA Guidance to LRFs:

As non-statutory bodies (LRFs are not a legal entity), LRFs themselves are therefore not obligated to respond to requests made under the FOI or EIR legislation.

However, LRFs are made up of a range of statutory bodies who are obliged to respond. Many LRFs have responded to FOI requests as a collective. Furthermore, the Environmental Information Regulations (EIR) is less prescriptive in which organisations it covers with the general principle that it applies to all organisations carrying out 'functions of public administration'.

It is usual practice for the lead organisation for the LRF to coordinate the response in collaboration with all relevant partners. However, where the partnership involves a large number of partners this may not enable compliance with the statutory timescale. For this reason, LRFs should make their own arrangements and document these as evidence of due diligence in enabling statutory requests for information. Please note the 20 working day limit for responding begins as soon as a request is received by a public authority.

If an LRF receives a request for information, it should pass this request on to its constituent members as soon as possible and notify the requester that it has received this request and passed it on to its members with the date on which they will receive a response.

LRFs will have varying policies for how they respond to these requests and their constituent members will themselves also have varying policies on how to respond.

Useful links for further information would be the Freedom of Information Act 2000 (FOI Act) and the Environmental Information Regulations 2004 (EIR) as they apply to LRFs

Purpose

The purpose of this document is to provide a framework of options for how the ERF will respond to an FOIA/EIR request received by the ERF Secretariat, either directly or via any partner within the forum.

Initial Action

On receiving an FOIA request, where the information/data being requested is held by the ERF Secretariat the request will be responded to by ECFRS FOI Team. Where the requested data is held by partners, ECFRS will share the request to all ERF partners for their information. ERF partners will then process any new request within their own organisational procedures, either disclosing or exempting data they hold, and advising where they do not hold the data where it may be available from, if known.

If received by the ERF Secretariat the following flow chart should be considered for each aspect of the FOI request:

Does the ERF Secretariat hold the data requested?

Yes

Does the ERF Secretariat own the data requested?

Yes – release data, subject to applicable exemptions

No – ERF Secretariat via ECFRS FOI Team provides a 'not held' response and advises the requester that ERF partners may hold some or all of the requested information, providing the FOI details for each partner and advising them to submit their request to the partners. All partners would then handle and respond to any new request within their own procedures.

No – The ERF Secretariat via ECFRS FOI Team provides a 'not held' response and advises the requester that ERF partners may hold some or all of the requested information, providing the FOI details for each partner and advising them to submit their request to the partners. All partners would then handle and respond to any new request within their own procedures.

If the request is received by a partner other than the Secretariat the following flow chart should be considered for each aspect of the FOI request:

Does the partner hold the data requested?

Yes

Yes – release data, subject to applicable exemptions using own internal procedures

No – Partner provides a 'not held' and advises the requester that the requested data may be held by ERF partners, providing their contact details, and advising them to submit their requests to the partners. All partners would then handle and respond to any new request within their own procedures.

→ **No** – Partner provides a 'not held' response and advises the requester that the requested data may be held by ERF partners, providing their contact details, and advising them to submit their requests to the partners. All partners would then handle and respond to any new request within their own procedures.

Summary

One or more of the following outcomes should form the basis of the agreed next steps at the initial meeting: [1]

- ERF Secretariat or partner (whoever receives the request) to release the information/data subject to FOIA applicable exemptions where it owns the data.
- If the data is not held it will advise the requester of this, and that they should submit their request to partners using the contact details provided. ERF partners will respond using their own internal procedures.
- Each partner can then make their own decision regarding disclosure or exemption of the data they hold or provide a 'not held' response; which will ensure responses are provided within the statutory timescale of 20 working days

Appendix B – List of Organisations (Name only) signed up to protocol

Basildon Borough Council
Braintree District Council
Brentwood Borough Council
British Transport Police
Castlepoint District Council
Chelmsford City Council

[1] *requirement throughout to protect personal data under GDPR and DPA 2018 regimes.*

Colchester Borough Council
East of England Ambulance
East Suffolk & North Essex NHS Foundation Trust
Epping Forest Council
Harlow District Council
Hertfordshire & West Essex Integrated Care Board
Maldon District Council
Mid and South Essex Foundation
Mid and South ICB
NELFT
Princess Alexandra Hospital
Provide
Rochford Council
Salvation Army
Southend City Council
Suffolk & North East Essex Integrated Care Board
Tendring District Council
Thurrock Council
Uttlesford District Council
Victim Support