WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement: Domestic Abuse Needs Assessment and Strategy Monitoring

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, Essex, CM1 1QH	08457 430430	DPO@essex.gov.uk	Paul Turner	Z6034810
Basildon District Council	Basildon Centre, The, St. Martins Square, Basildon, SS14 1DL	01268 533333	dpo@basildon.gov.uk	Sue Marriott	Z5361180
Braintree District Council	Causeway House, Bocking End, Braintree CM7 9HB	01376 552525	DPO@braintree.gov.uk	Kim Mayo	Z5103738
Brentwood District Council	Town Hall Ingrave Road Brentwood Essex CM15 8AY	01277 312500	dpo@evalian.co.uk	Evalian Limited	Z2092695
Castle Point Borough Council	Kiln Rd, Thundersley, Benfleet SS7 1TF	01268 882200	legal@castlepoint.gov.uk	Angela Hutchings	Z588703X
Chelmsford City Council	Civic Centre Duke Street Chelmsford Essex CM1 1JE	01245 606215	John.breen@chelmsford.gov.uk	John Breen	Z7829039
Colchester City Council	33 Sheepen Road Colchester Essex CO3 3WG	01206 282222	DPO@colchester.gov.uk	Nicola Cooke	Z5733593
Epping Forest District Council	Civic Offices High Street	01992 564000	lridley@eppingforestdc.gov.uk	Lynne Ridley	Z5033101

	Epping Essex CM16 4BZ				
Harlow District Council	Civic Centre, The Water Gardens, College Square, Harlow CM20 1WG	01279 446655	data.protection@harlow.gov.uk	Julie Galvin	Z7603332
Maldon District Council	Princes Road Maldon Essex CM9 5DL	01621 875749	dpo@maldon.gov.uk	Emma Holmes	Z6616948
Rochford District Council	Council Offices, South St, Rochford, Essex SS4 1BW	01702 546366	dpo@evalian.co.uk	Evalian Limited	Z6617133
Tendring District Council	Town Hall, Station Rd, Clacton-on-Sea CO15 1SE	01255 686060	dpaofficer@tendringdc.gov.uk	Judy Barker	Z577148X
Uttlesford District Council	London Road Saffron Walden Essex CB11 4ER	01799 510508	dpo@uttlesford.gov.uk	Tom Falconer	Z5060641

Version Control

Date Protocol comes into force	October 2023
Date of next Protocol review	October 2027
Protocol Lead Organisation	Essex County Council
Protocol drawn up by (Author(s))	Ana Dutu, Tom MacGregor, Essex County Council
Status– DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	0.1

Wider Eastern Information Stakeholder Forum

This Information Sharing Protocol (ISP) 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 you publish the ISPs you have signed up to with your online privacy notice.

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)	Domestic Abuse Needs Assessment and Strategy Monitoring 2024 #1246	**Essex County Council**
Supporting Standard Operating Procedure		
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

1 – Purpose

The Domestic Abuse Act received royal assent in April 2021. The legislation requires Tier 1 local authorities to:

- Appoint a multi-agency Domestic Abuse Local Partnership Board
- Assess the need for domestic abuse support within safe accommodation in their area for all victims, and their children
- Prepare and publish a strategy for the provision of such support
- Give effect to the strategy (through commissioning and decommissioning decisions)
- Monitor and evaluate the effectiveness of the strategy
- Report back annually to central government.

A first Needs Assessment was completed in 2021, based on which a Strategy was built and published, and a Partnership Board was established. There is however a requirement to refresh the needs assessment annually (with a full refresh needed at least every 3 years), to update the strategy in 2024, to monitor & evaluate the effectiveness of the strategy and to report back annually to central government. In order to achieve a complete refresh of the upcoming Needs Assessment, which would support with the updating of the Domestic Abuse Strategy, and for the Strategy monitoring duty to be fully fulfilled, the sharing of data on domestic abuse victims requiring housing support by Tier 2 local authorities is essential.

As such, the primary objective is to collect data captured on domestic abuse victims accessing housing support across the tier 2 authorities and analyse the shared data, which would:

- enable us to build a more accurate picture and a better understanding of the needs of domestic abuse victims and survivors in Essex;
- provides insight into the changes required to help further improve outcomes for domestic abuse victims and survivors;
- allow us to fulfil our duties under the Domestic Abuse Act 2021 of assessing the needs of domestic abuse victims in our area, build a Strategy which would address said needs, and monitor its effectiveness across the entire area.

In order to support us with achieving this objective, data will be provided by Basildon District Council, which will be analysed together with data from remaining Essex Tier 2 authorities, ECC data, Housing Providers data, and data collected from multiple external organisations which engage with and support victims of domestic abuse. The collection of the data and analysis will be undertaken by ECC. The data provided will solely be used for the purposes of the needs assessment, which will influence/support commissioning decisions and also for any evaluating of the effectiveness of commissioning decisions and reporting required back to DLUHC. A final report will be produced which will be shared with our DA Board and our local stakeholder. The Needs Assessment will be a public-facing document, which will be shared through the Essex Open Data platform. These reports will help with future commissioning intentions, to ensure we are funding services in the right areas as it will provide an overview of needs regarding numbers and demographics. We will also use the data alongside our performance monitoring as we have attached funding to the districts. To be clear, data will be shared by the districts to ECC, district data will not be shared with any other district.

2 – Information to be shared

Data to be shared is information as seen in the attachment below on Domestic Abuse victims who submitted a Homelessness Application to Basildon District Council. The shared data will be filtered prior to sharing for individuals whose Homelessness Application has the Main Reason for Loss of Settled Home recorded as Domestic Abuse. The information which will be shared is also captured in data fields in the Homelessness Case Level Information Collection (H-CLIC) data returns to the Department for Levelling Up, Housing and Community (DLUHC). Basildon District Council have also agreed to share additional data about the support services they provide to Domestic Abuse victims. Basildon District Council will extract this data (and the H-CLIC fields) directly from their own case management system. Only the data fields which are essential for the fulfilling of Domestic Abuse Act duties will be shared. The collection period required for the initial data transfer is April 2021-September 2023, with additional monitoring for new cases to occur on a quarterly basis.

Domestic Abuse Data - H-CLIC Fields.xlsx

Basildon_data_fields_DA_JSNA_2023.xlsx

3. Legal basis

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

Personal Data (identifiable data)	**Special Categories of Data (Sensitive identifiable data – if applicable)**	**Law Enforcement data (if applicable e.g. community safety)**
Article 6:	**Article 9: (if appropriate):**	**DPA Part 3 (if appropriate):**
Legal Obligation	**Substantial Public Interest DPA Schedule 1 Part 2 (6)(2)(a) (a)the exercise of a function conferred on a person by an enactment or rule of law.**	**Choose an item.**
Public Task	**Health & Social Care DPA Schedule 1 Part 1(2) (e) and Schedule 1 Part 1(2) (f)**	**Choose an item.**
Choose an item.	**Choose an item.**	**Choose an item.**
Choose an item.	**Choose an item.**	**Choose an item.**

Please list below relevant legislation or statute empowering this sharing activity:

Domestic Abuse Act 2021 Part 4 Section 57: Support provided by local authorities to victims of domestic abuse (1)Each relevant local authority in England must— (a) assess, or make arrangements for the assessment of, the need for accommodation-based support in its area, (b) prepare and publish a strategy for the provision of such support in its area, and (c) monitor and evaluate the effectiveness of the strategy.
The Care Act
The Children Act
The Domestic Violence Crime and Victims Act 2004,
Serious Crime Act 2015,
Stalking Protection Act 2019

4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as follows: **For help go to** Controllers and processors | ICO	**Tick box**	**Organisation Name(s)**
The Sole Data Controller (separate sole controllers) for this sharing is:	☒	**Essex County Council** **Each district council**
The Joint Data Controllers for this sharing are:	☐	
In the case of Joint Data Controllers, the designated single contact point for Individuals is:	☐	
Data Processors supporting the processing carried out under this protocol are (please list names):	☐	

Each organisation will remain the controller for the data they provide. Essex County Council will be controller for any combined datasets and outcomes derived from this. This Protocol will be reviewed 4 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

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. It is for the organisation initiating this ISP to identify which rights apply, and then each Partner has a legal responsibility to ensure they have the appropriate processes in place.

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.	☒
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.	☐ **N/A**
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 (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☐ **N/A**

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.	☒
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

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:

- ECC via SFTP (Secure File Transfer Protocol) – for the initial data transfer (April 2021- September 2023)
- Microsoft Azure Storage account, which will be set up for quarterly transfers (pending implementation by Technical Services)

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 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.

8. Format & Frequency

- The format the information will be shared in is **Excel spreadsheet/CSV**
- The frequency with which the information will be shared is **quarterly**

If a shared system is being used by partners:

- What system is being shared? **NA**
- Who is the owner of the system? **NA**

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.