**Information Sharing Protocol / Data Sharing Agreement**

# SUMMARY SHEET

**Title of Agreement: Hoarding Multidisciplinary Team (MDT)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organisation Name | Head Office Address | Phone | Email | Named Data Protection Officer | ICO Notification reference |
| Essex County Council | County Hall, Duke Street, Chelmsford, CM1 1QH | 08457 430430 | dpo@essex.gov.uk | Paul Turner | Z6034810 |
| Essex Police | New StreetEssex Police HQChelmsfordEssexCM1 1NF |  | dpo@essex.police.uk  | Michelle Watson | Z4883472 |
| Colchester Borough Homes | 1st Floor, Rowan House33 Sheepen RoadColchesterEssexCO3 3WG | 01206 508929 | dpo@colchester.gov.uk  |  | Z8259492 |
| Colchester Borough Council | 33 Sheepen RoadColchesterEssexCO3 3WG |  | dpo@colchester.gov.uk  |  | Z5733593 |
| Essex County Fire and Rescue Authority | Service HeadquartersLondon RoadRivenhallWithamEssexCM8 3HB | 01376 576265 | dpo@essex-fire.gov.uk    |  | Z5349761 |
|  Community360 | Winsley’s HouseHigh StreetColchesterEssex CO1 1UG | 01206505250 | tracyfortescue@community360.org.uk | Tracy Fortescue | ZA089382 |
| CVS Tendring | Imperial HouseRosemary RoadClacton-on-SeaEssexCO15 1NZ | 01255 425692 | Lisa.andrews@cvstendring.org.uk or admin@cvstendring.org.uk  | Lisa Andrews | Z5613025 |
| RCCE (Rural Community Council of Essex) | RCCE HouseThreshelfords Business Park.Inworth Road, FeeringCO5 9SE | 01376 574330 | sarah.sapsford@essexrcc.org.uk  | Sarah Sapsford | Z1011520 |
| St Helena | Myland Hall, Barncroft Close, Highwoods, Colchester, CO4 9JU | 01206 646 265 | dpo@sthelena.org.uk | David Traynier | Z7113713 |
| NEE H&W Alliance (ICB) | Endeavour House8 Russell Road, Ipswich, IP1 2BX | 01473 260 232 | dpo@snee.nhs.uk | Paul Cook | ZB340189 |
|  |  |  |  |  |  |

**Version Control**

|  |  |
| --- | --- |
| Date Protocol comes into force | September 2025 |
| Date of next Protocol review | September 2028 |
| **Protocol Lead Organisation** | Essex County Council (ECC) |
| Protocol drawn up by (Author(s)) | Gemma Gibbs, Senior Information Governance Officer |
| Status– DRAFT/FOR APPROVAL/APPROVED | APPROVED |
| Version  | 1.1 |

**Wider Eastern Information Stakeholders 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. 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) | 1121 | ECC (for ECC purposes only) |

1 – Purpose

|  |
| --- |
| The main purpose of the Multidisciplinary Team (MDT) is to prevent hoarding behaviours reaching safeguarding levels by ensuring the individual has access to all support available to them. The aim of the MDT is to provide specialist support and enhance outcomes and well-being for adults by inviting other services to discuss the needs of the individual and provide support where necessary. This will require the adult’s personal information to be shared between services to develop pro-active and sustainable case management plans, to prevent the risk of the adult’s situation worsening and requiring actions under safeguarding or enforcements through Environmental Health. For example, an adult can be evicted due to hoarding behaviours, which can lead to a higher risk for the adult.Essex County Council will share initial information with the organisations listed above for them to determine if they currently have contact with the individual, or if they have in the past. Information around the situation will also be shared to determine if the organisation is able to provide support. During the meeting the individual will be discussed, and additional information provided where needed and available. The meeting will take place over Teams and will not be recorded. In the event an organisation needs information to be sent to them in order to provide the support and fulfil their duties this will be sent via secure email. Each organisation will become sole data controller of the data they process due to having their own duties and purposes for processing. |

2 – Information to be shared

|  |  |  |
| --- | --- | --- |
| Organisation Name | Personal data fields | Special Category Personal Data fields |
| Essex County Council – prior to the meeting this information will be made available as Read Only on Sharepoint | Name | Situation regarding hoarding |
| Address |  |
| Date of Birth |  |
| During the meeting the situation will be discussed, this information may be shared | Marital status | Health needs/diagnosis |
| Members of the household | Any information relevant to the adult’s hoarding/situation |
| Keyholders | Religious or Philosophical beliefs |
| GP | Racial or ethnic origin |
| Homeowner details |  |
| NOK details |  |
| Organisations involved |  |
| After the meeting the above information may be shared with organisations that require it to enable them to perform their duties and/or provide support via secure email. |

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) |
| Article 6:  | Article 9: (if appropriate):  |
| Legal Obligation | Health & Social Care |
| Public Task | Substantial Public Interest |

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 [x]

Please list below relevant legislation or statute empowering this sharing activity: [Legislation guides | Local Government Association](https://www.local.gov.uk/parliament/legislation-guides)

|  |
| --- |
| Care Act (2014) |
| Mental Capacity Act 2005 |
| Mental Health Act 1983 |
| Public Health Act 1936 |
| Environmental Protection Act 1990 |
| Homelessness Reduction Act |
| Housing Act 2004 |
| For more information on legislation please see the Hoarding Guidance: |

4. Responsibilities

For help go to [Controllers and processors | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/)

|  |  |  |  |
| --- | --- | --- | --- |
| DATA CONTROLLERS - Organisation Name(s) | Data Protection Status | Provide Data | Access Data |
| All organisations named | Controller |[x] [x]

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.

|  |  |
| --- | --- |
| Data Subject RightsSelect the [applicable rights](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-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 privacy notices to support greater transparency.  | [x]  |
| UK GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner. | [x]  |
| UK GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.  | [x]  |
| 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. | NA |
| UK GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.  | [x]  |
| 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. | [x]  |
| 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. | [x]  |
| 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. | NA |
| 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. | [x]  |

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 information being sent via secure email and meetings taking place over Teams with only necessary partners being present.

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. Format & Frequency

* The format the information will be shared in is via read-only SharePoint initially, during Teams meetings and then be secure email if shareholders require information to perform their duties.
* The frequency with which the information will be shared is monthly.

If a shared system is being used by partners:

* What system is being shared? SharePoint for read only access.
* Who is the owner of the system? ECC
* A DPIA has been completed and approved for the use of this system YES

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

# 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 [x]

# 10. 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.

# 11. Complaint Handling

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

# 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 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.

# 14. Agreement

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