**WEISF INFORMATION SHARING PROTOCOL**

# SUMMARY SHEET

**Title of Agreement: Afghan Resettlement Programme – TB Screening**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organisation Name | Head Office Address | Phone | Email | Named Data Protection Officer | ICO Notification reference |
| Essex County Council | County Hall,Market Road,ChelmsfordEssex | 08457 430430 | dpo@essex.gov.uk  | Paul Turner | Z6034810 |
| North East Essex CCG | Aspen House,Stephenson Road,Colchester,Essex | 01206 918700 | Dpo.neeccg@nhs.net  | Paul Cook | ZA007604 |

**Version Control**

|  |  |
| --- | --- |
| **Date Agreement comes into force** | April 2022 |
| **Date of Agreement review** | April 2025 |
| **Agreement owner (Organisation)** | Essex County Council |
| **Agreement drawn up by (Author(s))** | Gemma Gibbs, Senior Information Governance Officer |
| **Status of document – DRAFT/FOR APPROVAL/APPROVED** | APPROVED |
| **Version**  | 1.0 |

**Wider Eastern Information Stakeholder Forum**

This Information Sharing Protocol is designed to ensure that information is shared in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

This protocol will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits include:

* transparency for individuals whose data you wish to share as protocols are published here;
* minimised risk of breaking the law and consequent enforcement action by the Information Commissioner’s Office (ICO) or other regulators;
* greater public trust and a better relationship by ensuring that legally required safeguards are in place and complied with;
* better protection for individuals when their data is shared;
* increased data sharing when this is necessary and beneficial;
* reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
* a better understanding of when, or whether, it is acceptable to share information without people’s knowledge or consent or in the face of objection; and reduced risk of questions, complaints and disputes about the way you share personal data.

Please ensure all sections of the template are fully completed with sufficient detail to provide assurance that the sharing is conducted lawfully, securely and ethically.

|  |  |  |
| --- | --- | --- |
| Item | Name/Link /Reference | Responsible Authority |
| Data Protection Impact Assessment (DPIA) |  |  |
| Supporting Standard Operating Procedure |  |  |
| Associated contract |  |  |
| Associated Policy Documents |  |  |
| Other associated supporting documentation |  |  |

Published Information Sharing Protocols can be viewed on the [WEISF Portal.](https://weisf.essex.gov.uk/)

1 – Purpose

|  |
| --- |
| The Home Office policy “Funding Instruction for local authorities in the support of the Afghan Citizens Resettlement Scheme (ACRS) and Afghan Relocation and Assistance Policy (ARAP)” sets out the scope for claims that can be made and incorporates a data sharing agreement with expectations about information sharing parameters.Afghan citizens, under the Resettlement Scheme, are entitled to TB screening. The CCG is unable to confirm whichGP practice an individual is registered with which means they are unable to contact them with details explaining how to book their screening appointment. Limited Personal Information will be provided by ECC to the NEE Continuing Health Care Team who have access to the NHS Spine. Using the PII they can identify which GP practice the individuals are registered with so that referrals into the screening provider can be achieved.This activity will be conducted in the Colchester/Tendring areas of the County.Instructions to the Data Processor (CCG/NEE Continuing Health Care Team).* The PII is only to be used for the purpose detailed above.
* The PII must not be shared with any third party not mentioned in the ISP.
* The PII must not be added to another dataset and used for another purpose.
* The PII must be stored securely until it is deleted.
* The PII must be deleted once the relevant check has been made and no longer than one week after receipt.

Please note that at this current time password protection will not be used on the document being shared. Secure email must be used.Essex County will not be receiving any personal information as part of this agreement.Section 1.8 of the Funding Agreement (including Data Sharing Agreement) sets out the responsibility of Essex County Council to ensure that Beneficiaries (Afghan citizens under the ACRS) are provided with a dedicated source of advice and support to assist with registering for mainstream benefits and services and signposting to other advice and information giving agencies. The support includes:s.1.8.4 Registering with a local GP, and other healthcare providers in line with identified medical needs.s.1.8.5 Advice around and referral to appropriate mental health services and to specialist services as appropriate. |

2 – Information to be shared

Essex County Council will provide the following information regarding Afghan citizens under the ACRS:

Full Name

Date of Birth

Full Address including post code

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) | Law Enforcement data (e.g. community safety partnerships) |
| Article 6:  | Article 9: (if appropriate): *N/A* | DPA Part 3 (if appropriate): *N/A* |
| Public Task | 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:

|  |
| --- |
| Funding Instruction for local authorities in the support of the Afghan Citizens Resettlement Scheme and Afghan Relocation and Assistance Policy (including Data Sharing Protocol) |

4. Responsibilities

|  |  |  |
| --- | --- | --- |
| 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: |[x]  Essex County 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 party to this protocol are (please list): |[x]  CCG |

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 Essex County Council, Resettlement Programme Manager.

5. Data Subject Rights

Partner Agencies’ Information Sharing Agreements are made publicly available on the Wider Eastern Information Stakeholder Forum website to enable compliance with article 12 of the GDPR.

It is each Partner’s responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. Partners will respond within one month of receipt of a notice to exercise a data subject right. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

|  |  |
| --- | --- |
| 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  |
| 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. | [x]  |
| GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner | [x]  |
| GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.  | [x]  |
| 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.  | [x]  |
| 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]  |
| 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. | [x]  |
| 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. | [x]  |
| 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. | [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 GDPR as applied by the Data Protection Act 2018.

The security of the personal data in transit will be assured by: Secure email will be used for the transfer of the information. The excel spreadsheet will not need to be password protected.

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.

7. International Transfers **- (Not applicable)**

# 8. Format & Frequency

* The format the information will be shared in is an excel spreadsheet
* The frequency with which the information will be shared is as required

If a shared system is being used by partners:

* What system is being shared? N/A
* Who is the owner of the system? N/A

# 9. Data Retention

Information will be retained by the Data Processor for no longer than one week. 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 [x]

# 11. Personal Data Breach Notifications

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 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 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.

# 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 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 is approved by the responsible person within each organisation (SIRO/Caldicott Guardian/Chief Information Officer).

**Please submit this Protocol to** **weisf@essex.gov.uk** **with a 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 at** [**https://WEISF.essex.gov.uk**](https://WEISF.essex.gov.uk)