**WEISF INFORMATION SHARING PROTOCOL**

# SUMMARY SHEET

**Title of Agreement:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organisation Name | Head Office Address | Phone | Email | Named Data Protection Officer | ICO Notification reference |
| Provide CIC | 900 The Crescent, Colchester, Essex, CO4 9YQ | 0300 303 9999 | [Provide.infogov@nhs.net](mailto:Provide.infogov@nhs.net) | Petra Lastivkova | Z2604172 |
| Essex County council (ECC) | County Hall, Market Road, Chelmsford, Essex, CM1 1QH | 0845 430430 | [DPO@essex-gov.uk](mailto:DPO@essex-gov.uk) | Paul Turner | Z6034810 |
|  |  |  |  |  |  |

**Version Control**

|  |  |
| --- | --- |
| **Date Agreement comes into force** | April 2022 |
| **Date of Agreement review** | April 2025 |
| **Agreement owner (Organisation)** | Provide |
| **Agreement drawn up by (Author(s))** | Helen McRorie (Provide) and Gemma Gibbs (Senior Information Governance Officer, ECC) |
| **Status of document – DRAFT/FOR APPROVAL/APPROVED** | APPROVED |
| **Version** | V1 |

**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 |
| Privacy Impact Assessment (PIA/DPIA) |  |  |
| Supporting Standard Operating Procedure |  |  |
| Associated contract |  |  |
| Associated Policy Documents |  |  |
| Other associated supporting documentation |  |  |

# 1 – Purpose

|  |
| --- |
| [The National Child Measurement Programme (NCMP](https://www.gov.uk/government/collections/national-child-measurement-programme)) is a nationally mandated public health programme. It provides the data for the child excess weight indicators in the Public Health Outcomes Framework and is part of the government’s approach to tackling child obesity. The Office for Health Improvement and Disparities provides strategic leadership and support for this programme, and local authorities deliver it.  The Child Health Information Service (CHIS) is an NHS commissioned service delivered by Provide. Their role is to ensure that information about a child’s school is available on TPP SystmOne to relevant clinicians including school nursing services, GPs and Specialist Children’s services and any other party involved in the child’s care. This data matching enables the necessary recording and uploading of data for the National Child Measurement Programme (NCMP).  In order to keep records up to date and accurate, Provide Child Health team (CHIS) is requesting information from Essex County Council. The purpose is to ensure that the CHIS service have an accurate record of children who have moved into borough but not listed as having a school or being home schooled.  **The benefits**  Both partners have accurate records resulting in a submission of up-to-date information to the NCMP.  Importantly the child health record held within local CHIS follows the child and family when they move GP or move area and provides a failsafe to ensure that all children, including those not registered with a GP, have been offered and have access to vital public health services. The role of the Local Authority is to provide the current school details under its duty to safeguard and help provide positive outcomes for children in Essex.  **Responsibilities of Essex County Council and Provide CHIS:**  Under the Children’s Act 2004, Section 10 it sets out the role of the local authority in improving the well-being of children in the authority’s area so far as relating to:   1. physical and mental health and emotional well-being 2. protection from harm and neglect.   Provide shares those responsibilities as a commissioned provider of the CHIS.  To enable the recording and uploading of data for the National Child Measurement Programme. |

# 2 – Information to be shared

|  |  |
| --- | --- |
| **Agency Name** Essex County Council (ECC) | **Data field/description** |
| **School Information** | School URN number  School Name  Childs Forename  Childs Surname  Date Of Birth  Address including postcode  School entry date  School leaving date  *NB Full postcode is required to ensure that all contact details on a child’s record are correct and that we have the correct child as there may be two children with the same name.* |
| **School Transfers (Infant to Junior school and Primary/Junior to Secondary school)** | Current school  New school  Child’s forename  Child’s surname  Date of birth  Address including postcode |
| **Reception year admissions** | School Name  Child’s forename  Surname  Date of birth |

# 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)** |
| **Article 6**: | **Article 9**: |
| Public Task | Health & Social Care |

Please list below other relevant legislation or statute below:

|  |
| --- |
| Children’s Act 2004, Section 10 & 11- Cooperation to improve well-being. |
| Children’s Act 1989. Part III: Section 17 (1) (provision of service) |
| Human Rights Act 1989 |

# 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: |  | Provide CIC, ECC |
| 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): |  |  |

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 Provide.

# 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 UK 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. 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.

|  |  |
| --- | --- |
| **Subject Rights**  **Select 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** | Processes are in place to enact this right - please check the box |
| 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. |  |
| 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. |  |
| 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: sending an excel spreadsheet via secure email.**

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. Format & Frequency

* The format the information will be shared in an **Excel Spreadsheet**
* The frequency with which the information will be shared is **annually in** **October and January.**

# 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. 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

# 10. 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 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.

# 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 Lead Partner at [Provide.infogov@nhs.net](mailto:Provide.infogov@nhs.net). The Lead Partner 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 has been approved by the responsible person within each organisation (SIRO/Caldicott Guardian/Chief Information Officer).