WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement: Access to the Child Health Information System for Safeguarding purposes

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Market Road Chelmsford, CM1 1QH	08457 430430	dpo@essex.gov.uk	Paul Turner	**Z6034810**
Provide	900 The Crescent, Colchester, CO4 9QB	01206 587370	john.adegoke@nhs.net	John Adegoke	Z2604172

Version Control

Date Protocol comes into force	May 2022
Date of next Protocol review	May 2025
Protocol Lead Organisation	Essex County Council
Protocol drawn up by (Author(s))	Gemma Gibbs, Senior Information Governance Officer (ECC)
Status– 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:

- 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	**NA**	
Associated contract	**NA**	
Associated Policy Documents		
Other associated supporting documentation		

1 – Purpose

ECC Children & Families have statutory duties under the Children Act 1989 to safeguard and promote the welfare of children. Under Section 11 of that Act, ECC Children & Families are required to provide a mechanism for professionals, families and members of the community to express any safeguarding concerns they have for children and for these to be reviewed and decisions made by a qualified social worker about what action, if any, is necessary to safeguard or promote the welfare of that child. Section 11 also sets out the duties and responsibilities of partner agencies to co-operate with ECC Children & Families Services and one form of co-operation would be the sharing of relevant and necessary information.

The Children & Families Hub provides a central point for safeguarding and welfare concerns about children to be received and reviewed in line with the legislative guidelines set out in the paragraph above. In order to properly review referred concerns the Children & Families Hub must know the identity of the child. In most cases those who share concerns with the Children & Families Hub provide sufficient information for the child to be accurately identified.

On a daily basis the Children & Families Hub receives concerns about children where there is limited and insufficient information available to identify the child and their parents. These concerns are often submitted anonymously or from concerned members of the public who do not know the identity of the child. In these instances, it is necessary to request cooperation from another partner agency who may hold information which would assist with the identification of a child.

At present, the Child Health Information System (CHIS) is the only record, within the broader children's services network, which centrally captures the personal details of children, across the full age range, who access universal health services and reside within the Essex County boundaries. Other agency databases for children accessing universal services are limited by age, geography and opt in/out arrangements.

It is therefore necessary for the Children & Families Hub to have frequent and timely 'as and when required' access to information held within the CHIS for the purposes of identifying children and contact details for their parent / carer where potential safeguarding and welfare concerns have been shared with ECC Children & Families Service. The information required is limited to the child and parent / carer's personal and contact details. Information about appointments, health needs or health professional's opinions is not required for the purposes of identifying the child and will not be recorded on the records created or held by the Children & Families Hub.

The Children & Families Hub will only record within its permanent records identifying information obtained from CHIS where it has been possible to accurately identify the child. Where more than one potential match of information is identified through CHIS the

Children & Families Hub will make additional enquiries to triangulate and clarify identity. Where it is not possible to accurately identify the child of concern no record of potential matches from CHIS will be made within Children & Families records.

2 – Information to be shared

- Name
- Address
- Contact Details
- Place and Date of Birth
- Ethnicity
- Record sharing preferences
- Groups and relationships
- Address history
- Registered and Previous GP
- School details
- Gender
- Sharing consent overrides
- Patient alerts – such as LAC, CP etc..

This will be for active records only.

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**
Vital Interests	**Substantial Public Interest**
Public Task	**Vital Interests**

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

Care Act 2014
The Children Act 1989-2004
Human Rights Act 1998
The Crime and Disorder Act 1998
Mental Capacity Act 2005
Learning and Skills Act 2000
Criminal Justice Act 2003
Working Together to Safeguard Children
Tackling Sexual Exploitation

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 for this sharing is:	☒	**Provide**
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):	☐	

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

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.	☐
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.	☐

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: *read only access to the CHIS system via N3 connection (or HSCN replacement)*

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.

7. International Transfers **NOT APPLICABLE**

8. Format & Frequency

- The format the information will be shared in is read only access to the TPP SystmOne Mid Essex CHIS unit via N3/HSCN replacement.
- The frequency with which the information will be shared is as and when required.

If a shared system is being used by partners:

- What system is being shared? TPP SystmOne
- Who is the owner of the system? Provide

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 has been 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.