

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. Chelmsford. CM1 1QH	033301 39824	informationgovernanceteam@essex.gov.uk	Gillian Furlong	Z6034810
PROVIDE	900 The Crescent. Colchester. CO4 9QB	01206 587370	Stephen.woodford@nhs.net	Stephen Woodford	Z2604172
NHS England – Eastern Region	Victoria House. Capital park. Fulbourn. Cambridge. CB21 5XE	01138 254987	peter.manser@nhs.net	Peter Manser	Z2950066
Version Control					
Date Agreement comes into force			9 th October 2017		
Date of Agreement review			9 th October 2018		
Agreement owner (Organisation)			Essex County Council		
Agreement drawn up by (Author(s))			Lauri Almond		
Status of document – DRAFT/FOR APPROVAL/APPROVED			FINAL		
Version			V1.0		

Whole Essex Information Sharing Framework

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		
Supporting Standard Operating Procedure	NA	
Associated contract	NA	
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the [WEISF Portal](#).

1.	Purpose	REFERENCES
	<p>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.</p> <p>Section 11 also sets out the duties and responsibilities of partner agencies in supporting ECC Children & Families in the discharge of their statutory safeguarding duties. It requires key 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.</p> <p>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 paragraphs 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.</p> <p>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 co-operation from another partner agency who may hold information which would assist with the identification of a child.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>	<p>GDPR Go to article 5</p>

CHIS the Children & Families Hub will make additional enquiries to triangulate and clarify identify. 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
Place and Date of Birth	Contact details
Ethnicity	Record sharing preferences
Groups and relationships	Address history
Registered and Previous G.P	School details
Gender	Sharing consent overrides
Patient alerts – such as LAC, CP etc...	

GDPR
Go to articles 6 - 9

This will be for *e* active records only.

3. Legal Basis

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the Data Protection Act 1998 Conditions for Processing (Schedules 2 & 3) **ONLY VALID UNTIL 25TH MAY 2018 at which point we will use the GDPR conditions in the 2nd table below.***

Personal Data	Sensitive Personal Data
Sharing personal information in accordance with this protocol is lawful under the <i>Data Protection Act 1998</i> Schedule 2:	Sharing personal information in accordance with this protocol is lawful under the <i>Data Protection Act 1998</i> Schedule 3: (if appropriate): <i>[please complete]</i> :
2 (6) - Legitimate Interests	3 (8) Medical Purposes
2 (4) - Vital Interests	2 (3) - Vital Interests
2 (5) - Administration of Justice/Public Functions	2 (7) - Administration of Justice/Enactment

Other legislation or statute as follows

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

GDPR
 Go to articles
 6-14

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the **General Data Protection Regulation 2016 (GDPR)**).*

Personal Data	Special Categories of Data
Sharing personal information in accordance with this protocol is lawful under the <i>General Data Protection Regulation 2016</i> article 6:	Sharing personal information in accordance with this protocol is lawful under the <i>General Data Protection Regulation 2016</i> article 9: (if appropriate): <i>[please complete]</i>
Public Task	Health & Social Care
Legal Obligation	Employment
Vital Interests	Vital Interests

Other legislation or statute as follows – as above

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.

Fair processing requirements have been satisfied by:

ECC’s privacy notice which references safeguarding processing can be accessed [here](#)

Provide’s privacy notice which references safeguarding processing can be accessed [here](#)

4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as:

√ or ×

Organisation Name(s)

GDPR
 Go to articles

The Sole Data Controller for this sharing is	√	Provide	13-14, 24 - 31
This Protocol will be reviewed one year after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by Essex County Council			
5. Subject Rights			
<p>GDPR Article 15 - Subject Access - is an individual's right to have a copy of information relating to them which is processed by an organisation.</p> <p>Once information is disclosed from one agency to another, the recipient organisation becomes the Data Controller for that information. With regards to subject access requests, the Data Controller has a statutory duty to comply with article 15 of the GDPR, unless derogation applies. It is good practice for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory derogation that may need to be applied prior to disclosure to the requesting individual. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory 20 working days (additional 2 months for complex SARs), time period.</p> <p>If a party receives a request for information under the Freedom of Information (FOI) Act 2000 or Environmental Information Regulations (EIR) 2004 that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, 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 under the provisions of the FOI Act or EIR 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.</p> <p>Essex Partner Agencies' Information Sharing Agreements are made publicly available on the Whole Essex Information Sharing Framework website to enable compliance with article 12 of the GDPR.</p> <p>GDPR Article 17 (1)(b)&(e) – Right to be forgotten – This right may apply where the sharing is based on consent, 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 to ensure compliance with the GDPR.</p>			<p>GDPR Go to articles 12 – 22</p> <p>GDPR Go to article 17 & 19</p>
6. Security of Information			
Control in place	√ / ×	GDPR	

There are good quality access control systems in place	√	articles 30 - 45
Paper information is stored securely	√	
Paper and electronic information is securely destroyed with destruction log for electronic information	√	
Laptops and removable media such as memory sticks are secured when not in use	√	
Technical security appropriate to the type of information being processed is applied	√	
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	√	
Disaster recovery arrangements are in place	√	
Encryption of personal data is fully implemented	√	
Data minimisation has been considered	√	
Can pseudonymised or anonymised data be used to meet your processing needs?	x	
There are sufficient access controls for systems/networks in place	√	
Routine and regular penetration tests are carried out	√	
Article 40 Codes of Conduct are adhered to (where applicable)	√	
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	√	
Additional control 1 – please specify here		
Additional control 2 – please specify here		
<p>Personal information will be securely shared via read only access to the CHIS system via N3 connection (or HSCN replacement)</p> <p>Partners receiving information will:</p> <ul style="list-style-type: none"> • 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 and Frequency	
<p>The format the information will be shared in is read only access to the TPP SystemOne Mid Essex CHIS unit via N3/HSCN replacement</p> <p>The frequency with which the information will be shared is as and when required</p>		
8.	Data Retention	
<p>Information will be retained in accordance with each partners' published data retention policy and in any event no longer than is necessary.</p>		<p>GDPR Go to article 5</p>
9.	Data Accuracy	
<p><i>(Detail how the organisation will ensure the accuracy of the information shared, how this will be achieved in accordance with GDPR article 5, and detail the process for correcting inaccurate data).</i></p> <p>The Provide Child Health team have a number of mechanisms in which data quality is assured in all Child records. TPP SystemOne is connected to the NHS Spine and therefore updates to demographic information including address and contact details are made available when changes are made in another care setting (for example if the Child's G.P makes an update to their record).</p> <p>The organisation works with providers of the 0 – 19 service across Essex to ensure that information held is accurate and up to date and is in the process of putting in place reciprocal agreements to ensure that Children are registered and are known to the relevant providers of the these services as well as ensuring that they are registered on the Child Health Information System.</p> <p>In the unlikely event that Essex Children's and Families Hub discovers inaccurate information recorded in a child's record as part of their investigations, the Provide Child Health team should be notified to make relevant enquiries and to correct the erroneous information.</p>		<p>GDPR Go to articles 5, 16 - 18</p>
10.	Breach Notification	
<p>Where a security breach linked to the sharing of data under this protocol is likely to adversely affect a data subject, Partners are required to inform all involved Partners 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</p>		<p>GDPR Go to articles 33, 34, 77 - 84</p>

	<p>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.</p> <p>All involved Partners should consult on the need to inform the Data Subject, 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.</p> <p>All Partners to this protocol 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.</p> <p>A processor is liable for any damage caused by processing, only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.</p>	
<p>11.</p>	<p>Complaints</p>	
	<p>Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.</p>	<p>GDPR Go to articles 16 – 22 & 77</p>
<p>12.</p>	<p>Commencement of Protocol</p>	
	<p>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.</p>	
<p>13.</p>	<p>Withdrawal from the Protocol</p>	
	<p>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.</p>	
<p>14.</p>	<p>Agreement</p>	

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

Approver Name	
Organisation Name	
Date of Agreement	

Please submit this Protocol to weisf@essex.gov.uk with an attached email of approval from the signatory. The Protocol will then be published on weisf.essex.gov.uk.

