INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Child Health Information System

Organisation Name	Head Office Address	Phone	Email	Named DPO	ICO Notification reference
Provide CIC	900 The Crescent, Colchester, Essex, CO4 9YQ	0300 303 9999	Provide.infogov@nhs.net	Stephen Woodford	**Z2604172**
Essex Partnership University NHS Foundation Trust (EPUT)	Trust Head Office The Lodge Lodge Approach Runwell Wickford Essex SS11 7XX	0300 123 0808	epunft.info.gov@nhs.net	Lara Brooks	**ZA242481**
All Essex Schools **(Listed Separately at Appendix 2)**					

Version Control	
Date Agreement comes into force	01 April 2019
Date of Agreement review	01 April 2022
Agreement owner (Organisation)	Provide
Agreement drawn up by (Author(s))	Stephen Woodford, IG and IT Projects Manager
Status of document – DRAFT/FOR APPROVAL/APPROVED	FOR APPROVAL
Version	V1

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 (PIA/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.

1.	Purpose	REFERENCES
The agreement is necessary to ensure that children in Essex continue to receive the health services that they are entitled to and are not placed at risk by allowing the correct health professionals to be engaged in their health care in order to: • Improve the life circumstances and outcomes of children, young people and their family members; • Reduce the number of children and young people whose life circumstances and experiences make them at risk of harm; • Improve readiness of children for school In particular the Provide Child Health team requires information to ensure that a school for each school age child is recorded and updated on its system so that all eligible children are offered the National Child Measurement Programme and other screening services as directed by the Department of Health; The EPUT immunisation Team require this information to ensure school immunisation programmes are arranged and immunisation programmes are followed. The risk of not having an up to date child health record is that adequate health, education or social work services may not be provided. This agreement will ensure that: • Children with no school allocated to them are updated on the CHIS System (TPP SystmOne) • Children's records, moving into or out of the area are transferred/requested and accounted for in a timely manner. • That all children living or attending school within area have an electronic Child Health Record The timely provision of the vision, hearing, height & weight and immunisation screening programme carried out in schools	GDPR Go to article 5

2. Information to be shared

GDPR
Go to articles 6 - 9

Agency Name: Essex Schools	Data field/description
School Information	• School URN number • School name • Child's forename • Child's Surname • Date of birth • Gender • Address including postcode • School entry date • School leaving date
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 • Gender • Address including postcode
Reception year admissions	• School Name • Child's forename • Surname • Date of birth • Gender

3. Legal Basis

GDPR
Go to articles 6-14

General Data Protection Regulation 2016 (GDPR) and 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): NOT APPLICABLE	**DPA Part 3** (if appropriate): NOT APPLICABLE

Public Task	Choose an item.	Choose an item.
Legal Obligation	Choose an item.	Choose an item.

Other legislation or statute as follows:
Children's Act 2004, Section 10 & 11- Cooperation to improve well-being.
Children's Act 1989. Part III: Section 17 (1) (provision of service)

4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

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:	☐	
The Joint Data Controllers for this sharing are:	☒	
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Provide
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. Subject Rights

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.

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 for this sharing according to the legal basis you are relying on**	Processes are in place to enact this right - please check the box	GDPR Go to articles 12 – 15
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.	☒	
GDPR Article 15 – **Right of Access** – Individuals have the right to request access to the information about them held by each Partner	☒	
GDPR Article 16 – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	☒	
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.	☒	
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 restrict, unless it involves disproportionate effort.	☒	GDPR Go to article 16 & 22
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.	☐	
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

Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
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?	☐ **NA**	
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)	☐ **NA**	
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	☒	
Confirm entry in Records of Processing Activity	☒	
Additional measure 1 – Provide & EPUT are Cyber Essentials Plus and ISO27001 Accredited.	☒	

Personal information will be securely shared via Encrypted Email. It is recognised that schools do not routinely have

access to an encrypted email account therefore to facilitate this the Provide Child Health team will send a manually encrypted email from provide.childhealth@nhs.net to each of the schools party to this agreement. Each school will need to perform a one-time registration on the NHS Mail Encryption portal. Each school can then reply to the email through the NHS Mail encryption portal to send the information back securely.*

**Instructions for accessing NHS Mail Encrypted Emails are detailed in Appendix 1. A quick guide is also being developed by the Provide IG team which will be distributed to schools.*

No data can be shared via unsecure standard email.

No personal data will be transferred outside of the uk.

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.

International Transfers (NOT APPLICABLE AS NO DATA IS HELD OUTSIDE THE UK)

If any personal data is to be transferred outside of the EEA, please ensure you capture the relevant supporting adequacy decision for such a transfer here (articles 40-43).

Adequacy Decision in place https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en	Date of approval by EU Commission is:	[Provide hyperlink here]
ICO Approved standard contract clauses in place	Date of approval by ICO is:	[Provide hyperlink here]

https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf		
ICO Approved Binding Corporate Rules in place https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/	Date of approval by ICO is:	[Provide hyperlink here]
The Individuals have given explicit consent to the transfer and understand the risks associated with the transfer	Confirm this consent has been recorded appropriately	√ / ×
The receiving organisation in a 3rd country is bound by an approved Code of Conduct recognised by the EU	Date of approval by ICO is:	[Provide hyperlink here]

ICO guidance on International Transfers can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

7. Format and Frequency

The format the information will be shared in is **Excel Spreadsheet**

The frequency with which the information will be shared is **Monthly.**

Information obtained will be input onto the relevant Child's health record on TPP SystmOne.

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.

GDPR
Go to article 5

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 ☒

GDPR
Go to articles 5, 16 - 18

10. Breach Notification

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.		GDPR Go to articles 33, 34, 77 - 84
11.	**Complaints**	
Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.		GDPR Go to articles 16 – 22 & 77
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 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 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 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 on WEISF.essex.gov.uk

Appendix 1 – NHS Mail Encryption – Instructions for Recipients

Accessing+Encrypted+Emails+Guide.pd

Appendix 2 – schools list

Copy_of_All_Essex_
Schools_from_ECC_M