

WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET



Title of Agreement: ECC Education Compliance and CHIS ISP

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, Essex, CM1 1QH	0345 743 0430	dpo@essex.gov.uk	Paul Turner	Z6034810
Provide	900 The Crescent, Colchester Business Park, Colchester, Essex, CO4 9YQ	07817023237	Provide.infogov@nhs.net	John Adegoke	Z2604172

Version Control

Date Agreement comes into force	May 2021
Date of Agreement review	May 2024
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Anita Patel-Lingam
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	0.1

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		

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

1 – Purpose

The sharing of information between Essex County Council (ECC) and Essex and East Anglia Child Health Information Service (CHIS) has been identified as crucial in the interests of safeguarding children and young people who have been reported ‘missing from education’ and whose whereabouts cannot be confirmed via alternative available methods of investigation. The Data Protection Act 2018 and UK General Data Protection Regulations (GDPR) do not prevent the sharing of information for the purposes of keeping children safe.

Local authorities have a duty under section 436A Education Act 1996 to make arrangements to establish the identities of children in their area who are not registered pupils at a school and are not receiving suitable education otherwise. This duty only relates to children of compulsory school age. Parents have a duty, under section 7 Education Act 1996, to ensure that their children of compulsory school age are receiving suitable full-time education.

Where ECC receives information which indicates that a child may be ‘missing’ from education, we seek to make use of all available intelligence to enable us to respond swiftly and to return a child to suitable educational provision without delay. In order for statutory legal intervention to be pursued, it is essential that ECC is able to confirm the address at which those with parental responsibility for an identified child/young person reside. For this reason, this ISP is necessary to ensure that information held by ECC is cross-referenced against records held by CHIS, so that where any details have been updated within the CHIS database (e.g. where a family has moved address and/or registered with an alternative GP), such details can be shared to enable ECC to act, in the interests of safeguarding, with the most up-to-date contact information for the family.

The process by which information will be shared between both parties is as follows:

- ECC (Education Compliance team) will send agreed information, via secure email to a specified, secure email address managed by Provide.
- Provide colleagues, who have been granted access to the secure mailbox, will cross-reference the data held by CHIS and send a response back to ECC, via secure email, detailing any new updated contact details held within the database OR confirming that no alternative details are available.
- ECC Education Compliance team will make use of any updated contact details held for the family to continue their investigations and ensure that the local authority’s statutory duties in respect of ‘Children Missing Education’ are fulfilled.

2 – Information to be shared

Agency Name	Data field/description
Essex County Council – Education Compliance Team	Name s) of child/ren who have been reported as missing
	Date(s) of birth of child/ren concerned
	Last known address (held on school/ECC file)
	Previous School attended
	Unique Pupil Number
Child Health Information Service	Updated address details held on CHIS records
	Updated contact information held on CHIS records
	Updated school details held on CHIS records

N.B. If the same data is shared by each Partner then only complete once to cover all Partners. Please delete any unused lines

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:	DPA Part 3 NOT APPLICABLE
<i>Public Task</i>	Health & Social Care	Choose an item.

Please list below other relevant legislation or statute below:

Section 436A Education Act 1996
Section 7 Education Act 1997
Education (Pupil Registration) (England) (Amendment) Regulations 2016, Regulation 4

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:	<input checked="" type="checkbox"/>	Essex County Council Provide
The Joint Data Controllers for this sharing are:	<input type="checkbox"/>	
In the case of Joint Data Controllers , the designated single contact point for Individuals is:	<input type="checkbox"/>	
Data Processors party to this protocol are (please list):	<input type="checkbox"/>	

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 Essex County Council

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. 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.

<p>Subject Rights</p> <p>Select the applicable rights for this sharing according to the legal basis you are relying on</p>	Processes are in place to enact this right - please check the box
--	---

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.	<input checked="" type="checkbox"/>
GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner	<input checked="" type="checkbox"/>
GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	<input checked="" type="checkbox"/>
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.	<input type="checkbox"/>
GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>
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.	<input type="checkbox"/>
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.	<input checked="" type="checkbox"/>

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:

- Each secure email will only contain the relevant information about one individual
- There will be no personal identifiable information in the subject header of the email
- The email will be sent to the agreed recipient secure email and no other without prior agreement

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.

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 & Frequency

- The format the information will be shared in is via secure email. One email will be sent per family for whom cross-referencing checks have become necessary
- The frequency with which the information will be shared is daily, during peak periods (e.g. start of the new academic year, during school term time), We would anticipate that we could send (on average) 15 secure emails per week during peak periods. During school closure periods, we anticipate that (on average) we may send 3 secure emails per week.
- 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**

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. Provide will delete the secure email containing personal details provided for the matching once they have completed the match and notified the ECC Education Compliance Team.

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 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 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 <https://WEISF.essex.gov.uk>