

WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET



Title of Agreement: Teenage Pregnancy

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council (ECC)	County Hall, Chelmsford, Essex, CM1 1QH	0345 743 0430	dpo@essex.gov.uk	Paul Turner	Z6034810
The Princess Alexandra Hospital Trust (PAH)	First Floor, Kao Park 2 London Road Harlow Essex CM17 9NA	0127 996 2533	Paht.dpo@nhs.net	Tracy Goodacre	Z8759485

Version Control

Date Agreement comes into force	February 2022
Date of Agreement review	February 2025
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Gemma Gibbs (Senior IG Officer) and Helen Gregory (Wellbeing and Public Health Manager)
Status– DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	1.0

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
Data Protection Impact Assessment (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

Essex County Council Public Health team leads a multi-agency effort to reduce unwanted pregnancies among under 18's. Outcomes for teenage parents are disproportionately poor and contribute to intergenerational inequalities. To reduce teenage conceptions a system wide approach is required and accurate up to date data at a local level is key.

Public Health England U18 teenage conception and abortion data sets available to support this work are always a minimum of 2 years behind making it challenging for ECC and partners to effectively target prevention efforts. Covid has added an additional delay and presented wider challenges with regards to under 18 conceptions and abortions. As a result, there is now a growing need for live local data sets to support the activity of the Essex Teenage Pregnancy Prevention Group and wider Children, Families and Education partners. The collective analysis of a range of data sets from several commissioners and providers will support local knowledge, inform local quadrant Stay Safe Boards for supporting efforts in this area of work at community level and support wider county efforts including ensuring any funding is targeted appropriately.

Organisations involved in the Teenage Pregnancy Prevention work include Essex County Council Public Health, Essex Sexual Health Services (Provide), Essex Child and Family Wellbeing Service (Virgin Care and Barnardo's), Maternity Services, 5 x Clinical Commissioning Groups, District Councils, Brook, Essex Youth Service and Essex Children and Social Care.

The County Wide Teenage Pregnancy Prevention Group reports as required to Essex Health and Wellbeing Board. Teenage Pregnancy will be a standing item at quadrant Stay Safe Groups and feed back up to Essex Children's Safeguarding Board as required.

The data set provided will be collated and analysed by ECC Public Health Senior Analysts providing quarterly quadrant reports at district level on teenage conceptions and booking appointments, births, abortions (clinic and hospital) and access to sexual health services including a range of contraception methods – eC-Card, GP prescribed contraception, LARC, over the counter contraception. The reports will be shared with all partners who have provided data sets, members of local Stay Safe Boards and Essex Teenage Pregnancy Prevention Group and any other partners at a local level for whom it is relevant in support efforts to promote healthy relationships and prevent U18 conceptions. In addition, the data will support the forward planning to ensure teenage parents are able to access appropriate support as they require it.

2 – Information to be shared

Princess Alexandra Hospital will provide the following for the Under 18s:

- Date of booking
- Age at booking
- Partial Postcode (first half (outbound))
- Estimate of due date
- Involvement with social care
- Referral to social care
- Date pregnancy ended
- Outcome of pregnancy (e.g. miscarriage, registerable, termination)
- Date and time of delivery
- Mothers age at delivery
- Gestation Now

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
Public Task	Health & Social Care	Choose an item.

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

<p>LGA and PHE Teenage Pregnancy Prevention Framework states; <i>Strong use of data for commissioning and monitoring of progress</i> <i>Strong use of data is essential for assessing need, planning, commissioning and monitoring; and can enable proactive and targeted approaches. Data should be reviewed at all relevant levels (local authority, ward, LSOA etc) to establish variations and expose inequalities that may be masked by presentation of data at higher levels. Benchmarking appropriately (national, regional and statistical) enables relative progress to be monitored. Proxy data and indicators from local abortion and maternity providers can provide more timely monitoring of progress in addition to annual/quarterly ONS data. Data should be combined with local intelligence, and appropriately shared with local stakeholders, to inform commissioning decisions. For example, a school located in a high rate area may not be attended by young people from that community - targeted work with a neighbouring school attended by the majority of pupils from the high rate area would have greater impact. Collection of service data should be used to evaluate impact of commissioned programmes</i></p> <p>Teenage Pregnancy Prevention Framework (publishing.service.gov.uk)</p>
<p>NHS Act 2006 – Section 6 – Local Authority public health functions</p>

4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as follows:	Tick box	Organisation Name(s)
--	----------	----------------------

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.		
The Sole Data Controller for this sharing is:	<input checked="" type="checkbox"/>	Essex County Council Princess Alexandra Hospital
The Joint Data Controllers for this sharing are:	<input type="checkbox"/>	Not applicable
In the case of Joint Data Controllers, the designated single contact point for Individuals is:	<input type="checkbox"/>	Not applicable
Data Processors party to this protocol are (please list):	<input type="checkbox"/>	Not applicable

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 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. Partners will respond within one month of receipt of a notice to exercise a data subject right. 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 style="text-align: center;">Data Subject Rights</p> <p style="text-align: center;">Select the applicable rights for this sharing according to the legal basis you are relying on</p>	<p style="text-align: center;">Check box to confirm processes are in place</p>
<p>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.</p>	<input checked="" type="checkbox"/>
<p>GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner</p>	<input checked="" type="checkbox"/>
<p>GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.</p>	<input checked="" type="checkbox"/>
<p>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.</p>	<input type="checkbox"/>
<p>GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.</p>	<input checked="" type="checkbox"/>
<p>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.</p>	<input checked="" type="checkbox"/>
<p>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.</p>	<input checked="" type="checkbox"/>
<p>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.</p>	<input checked="" type="checkbox"/>
<p>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.</p>	<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 sending the information by secure TLS email to ensure encryption.

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. International Transfers – NOT APPLICABLE

8. Format & Frequency

The format the information will be shared in is in an excel spreadsheet sent by secure email to public.health@essex.gov.uk.

- The frequency with which the information will be shared is quarterly.

If a shared system is being used by partners: NOT APPLICABLE

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. 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 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 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 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.

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