INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Early Intervention Service User Tracking

Organisation Name	**Head Office Address**	**Phone**	**Email**	**Named Data Protection Officer**	**ICO Notification reference**
Essex County Council	County Hall. Chelmsford. Essex. CM1 1QH	033301 39824 300 555 1200	informationgovernanceteam@essex.gov.uk	Paul Turner	Z6034810
EWMHS	NELFT NHS Foundation Trust CEME Centre – West Wing Marsh Way Rainham Essex RM13 8GQ	0300 555 1200	Robert.Paley@nelft.nhs.uk	Robert Paley	Z9096541

Version Control	
Date Agreement comes into force	29/10/2020
Date of Agreement review	29/10/2023
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Wendy Pope and Kim Gisby
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	V0.1

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)	00413a	Essex County Council
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
Essex County Council are to invest £1,000,000 over two years, April 2020- March 2022, to extend the Early Intervention, Family innovation Fund (FiF). This fund supports children, young people and their parents/carers, providing specialist early intervention services for complex family needs. Further, as part of the early intervention response to COVID-19, some additional services have been commissioned within the same broad offer (FIF-Xtra Services) to support children and families experiencing anxiety specifically due to COVID-19. These services are at a value of £120,000 from June 2020 – June 2021. The business case requires that a percentage of service users are tracked over a five-year period, to show that these services prevent intervention from statutory services. The purpose of the evaluation is to build on the existing evidence base that Early Help works, specifically to: • Evidence what Early Help works, for who and why • Quantify the individual outcomes achieved and evidence their sustainability • Identify reduction in demand for more costly statutory intervention • Identify and estimate costs avoided through early intervention • Identify and estimate benefits of social return on investment ECC require information relating to individuals to show if there is a use of statutory services including: Emotional Wellbeing and Mental Health Service (EWMHS) Family Solutions (ECC) Youth Offending Teams (YOTS) (ECC) Education Welfare Services (ECC) Social Care (ECC) The learning captured by the evaluation will be used to inform future commissioning activities and to evidence the case for greater investment in Early Help both in Essex and nationally. This will not be used for decision making about individual service users. Individuals will provide consent to take part in this evaluation, all participants will be provided with information about what information will be collected and that their services will be tracked over the specified period. Please see the	GDPR Go to article 5

embedded consent form below which is to be given to individuals (see form below). If an individual does not consent this will not affect the service, they receive and individuals have the right to withdraw their consent at any time. A consent process is in place which includes how individuals requesting to withdraw their consent is managed and acted upon to stop processing personal data for those individuals.

The tracking will begin May 2020 with information being gathered every three months until March 2027. The individuals Name and Date of Birth will be shared with the statutory service to gather whether or not people who have had a FiF intervention have been referred to a statutory service(s).


FIF Consent Form July 2020.doc


FIFXtra referral and consent form v3.docx

2. Information to be shared

GDPR
Go to articles 6 - 9

Agency Name	Data field/description
Essex County Council	Name, D.O.B
• Emotional Wellbeing and Mental Health Service (EWMHS)	Whether or not people who have had a FiF or FIF-Xtra Intervention have, after that intervention, been referred to a statutory service(s). Why the individual was referred and how long they used the service for.

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): ***[please click and select]***	**DPA Part 3** (if appropriate): *[please click and select]*
Consent	Explicit Consent	Choose an item.
Choose an item.	Choose an item.	Choose an item.
Choose an item.	Choose an item.	Choose an item.

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:	☒	Essex County Council and EWMHS (NELFT)
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Essex County Council
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 Essex County Council.

5. Subject Rights

Essex 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.

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?	☐	
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	☒	
Confirm entry in Records of Processing Activity	☐	
Any risks associated with this data sharing have been assessed by your organisation and approval to proceed granted by your authorising signatories	☒	
Full consent process established including managing withdrawal of consent	☒	

Additional measure 2 – please specify here	☐

Personal information will be securely shared as an Excel Spreadsheet via secure email.

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. Format and Frequency

- The format the information will be shared in is an Excel spreadsheet via secure email.
- The frequency with which the information will be shared is every three months.

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