

# WEISF INFORMATION SHARING PROTOCOL

## SUMMARY SHEET



### Title of Agreement: Emotional Wellbeing Mental Health Service (EWMHS)

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
<b>Essex County Council</b>	County Hall, Chelmsford, CM1 1QH	08457 430430	<a href="mailto:IGTeam@essex.gov.uk">IGTeam@essex.gov.uk</a>	Paul Turner	<b>Z6034810</b>
<b>North East London Foundation Trust</b>	Goodmayes Hospital. Informatics Dept. Barley Lane, Ilford, IG3 8XJ	0300 5551201 ext. 64393	<a href="mailto:rpaley@nhs.net">rpaley@nhs.net</a>		<b>Z9096541</b>
<b>Southend Borough Council</b>	Civic Centre, Victoria Ave, Southend, SS2 6ER	01702 215000			<b>Z6929331</b>
<b>Thurrock Council</b>	Civic Offices, New Road, Grays, RM17 6SL	01375 652652			<b>Z8228055</b>

#### Version Control

<b>Date Agreement comes into force</b>	April 2021
<b>Date of Agreement review</b>	February 2022
<b>Agreement owner (Organisation)</b>	Essex County Council
<b>Agreement drawn up by (Author(s))</b>	ECC Information Governance Team
<b>Status of document – DRAFT/FOR APPROVAL/APPROVED</b>	APPROVED
<b>Version</b>	V1.1

# 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)	PIA 303	ECC
Supporting Standard Operating Procedure	NA	
Associated contract	EWMHS	WECCG
Associated Policy Documents	NA	
Other associated supporting documentation	NA	

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

# 1 – Purpose

The C&YP EWMH Partnership is delivering the service and the partnership covers Health's 7 CCGs, Essex County Council, Southend Council, Thurrock Council and NHS England.

The vision of this partnership is to improve the EWMH of children and young people, aged 0-25, with these needs. The aim being to improve their educational and social life chances by ensuring easy access and the provision of high quality services that use evidence-based effective interventions through the procurement of a newly integrated Tier 2 & 3 C&YP EWMH service. ECC and the CCGs have a joint statutory responsibility for the provision of Emotional Wellbeing and Mental Health Services for children and young people in Essex.

The parties have agreed that NELFT, ECC, TC and SBC are both Data Controllers in Common and that this is the necessary position in order to be compliant with information governance requirements for the Local Authority.

The contract was signed, subject to a side note to say that the issue needed to be resolved, although the contract states that, other than for very limited purposes, NELFT is the only authority which is Data Controller. It was always noted that the parties were not in agreement that this was the true legal position.

The statutory definition of Data Controller is 'a person who (either jointly or in Common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.'

The legal position relating to local authorities' sets out that the Local Authority has the right to determine, the purposes for which and the manner in which personal data are processed. This is because Local Authorities have the right to decide how complaints are handled. This is a non-delegable statutory duty which is inherent in Local Government law. Section 26(1) of the Local Government Act 1974 makes it clear that the Council has to retain full accountability for all services which it is the Council's function to provide. All services are provided as part of the council's functions. The Local Government Ombudsman has expressed concerns about Local Authority failures to contract appropriately.

Therefore, this protocol is to set out the purposes for which the parties now agree that ECC/SBC/TC are the data controller and the circumstances where ECC/SBC/TC will need access to personal data in order to meet its statutory obligations

# 2 – Information to be shared

The information to be shared is broadly those data items listed below, however the list is not exhaustive as the data required will be determined by the reason for access. The sharing of data will be carefully considered on a case by case basis and strictly limited to the minimum required to fulfil the justified purposes of sharing of such data.

- **Name (will be provided if known from ECC/SBC/TC and presented to NELFT otherwise it will be the be the below information only)**
- **Date of Birth**

- **Service Provision Dates**
- **Current care pathway**
- **Complaints information (NELFT will always seek consent where possible before releasing complaints information as part of best practice)**

N.B. Full access to clinical notes, created and managed by NELFT, is not required. Only a certain, limited data is required for specific purposes, to enable ECC/TC/SBC to fulfil their statutory duties. The specific purposes include verification of the identification of an individual, dates of their access to services and their care pathway

The reasons for access are likely to be:

- To respond to Local Government Ombudsman complaints;
- to respond to legal challenges, and;
- any other circumstances when we need to access the data to perform statutory functions.
- .

### 3. Legal basis

The identified conditions for processing under the Data Protection Act 2018:

<b>Personal Data (identifiable data)</b>	<b>Special Categories of Data (Sensitive identifiable data)</b>	<b>Law Enforcement data (e.g. community safety partnerships)</b>
<b>Article 6:</b> <i>[please click and select]</i>	<b>Article 9:</b> (if appropriate): <i>[please click and select]</i>	<b>DPA Part 3</b> (if appropriate): <i>[please click and select]</i>
<i>Consent</i>	Substantial Public Interest	Choose an item.
<i>Public Task</i>	Health & Social Care	Choose an item.
<i>Legal Obligation</i>	Explicit Consent	Choose an item.
Choose an item.	Choose an item.	Choose an item.

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

Fair processing requirements have been satisfied by: each data controller is responsible for the issuing of a privacy notice so that all data subjects are aware of how and when their data is processed.

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

Children’s Act 1975, 2004
Education and Skills Act 2008
The Health and Social Care Act 2012
Children and Families Act 2014
Mental Health Act 2007
Mental Capacity Act 2005
Local Government Act 1974

## 4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as follows: For help go to <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&amp;from=EN">https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&amp;from=EN</a> Articles 24 – 29 where these roles are explained.	Tick box	Organisation Name(s)
The Sole Data Controller for this sharing is:	<input type="checkbox"/>	
The Joint Data Controllers for this sharing are:	<input checked="" type="checkbox"/>	
In the case of <b>Joint Data Controllers</b> , the designated single contact point for Individuals is:	<input checked="" type="checkbox"/>	North East London Foundation Trust
Data Processors party to this protocol are (please list):	<input type="checkbox"/>	

This Protocol will be reviewed one year 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 **the Information Governance Team - ECC**

# 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 style="text-align: center;"><b>Subject Rights</b></p> <p style="text-align: center;"><b>Select the applicable rights for this sharing according to the legal basis you are relying on</b></p>	<p>Processes are in place to enact this right - please check the box</p>
GDPR Article 13&14 – <b>Right to be Informed</b> – 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 – <b>Right of Access</b> – Individuals have the right to request access to the information about them held by each Partner	<input checked="" type="checkbox"/>
GDPR Article 16 – <b>Right to Rectification</b> – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	<input checked="" type="checkbox"/>
GDPR Article 17 (1)(b)&(e) – <b>Right to be forgotten</b> – 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 – <b>Right to Restriction</b> – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	<input checked="" type="checkbox"/>
GDPR Article 19 – <b>Notification</b> – 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 type="checkbox"/>
Article 21 – <b>The Right to Object</b> – 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 – <b>Automated Decision-Making including Profiling</b> – 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"/>
<b>Freedom of Information (FOI) Act 2000</b> or <b>Environmental Information Regulations (EIR) 2004</b> 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 it being shared via secure TLS email systems

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 3<sup>rd</sup> party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

## 7. Format & Frequency

- The format the information will be shared in is **electronic text report form**
- The frequency with which the information will be shared is **as and when the need arises for the sharing**

If a shared system is being used by partners:

- What system is being shared? **NA**
- Who is the owner of the system? **NA**

## 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.

## 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](mailto: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](mailto:weisf@essex.gov.uk) with list of approved signatories. The Protocol will then be published on [weisf.essex.gov.uk](https://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>**