

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
Essex County Council	County Hall. Chelmsford. Essex. CM1 1QH	03457 430430	informationgovernanceteam@essex.gov.uk	Z6034810	County Hall. Chelmsford. Essex. CM1 1QH
North East London Foundation Trust	Goodmayes Hospital. Informatics Dept. Barley Lane. Ilford. IG3 8XJ	0300 5551201 ext. 64393	rpaley@nhs.net	Z9096541	North East London Foundation Trust
Southend Borough Council	Civic Centre. Victoria Ave. Southend. SS2 6ER	01702 215000		Z6929331	Southend Borough Council
Thurrock Council	Civic Offices New Road, Grays, RM17 6SL	01375 652652		Z8228055	Thurrock Council

Version Control	
Date Agreement comes into force	01/07/2017
Date of Agreement review	01/07/2018
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Lauri Almond
Status of document – DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	V1.0

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 303	ECC
Supporting Standard Operating Procedure	NA	
Associated contract	EWMHS	WECCG
Other associated supporting documentation	NA	

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

1.	Purpose	REFERENCES
	<p>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.</p> <p>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.</p> <p>The parties have agreed that NELFT and ECC 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.</p> <p>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.</p> <p>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.’</p> <p>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.</p> <p>Therefore, this protocol will is to set out the purposes for which the parties now agree that ECC/SBC are the data controller and the circumstances where ECC/SBC will need access to personal data in order to meet its statutory obligations</p>	<p>GDPR Go to article 5</p>
2.	Information to be shared	
	<p>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.</p> <ul style="list-style-type: none"> • Name (will be provided if known from ECC and presented to NELFT otherwise it will be the be the below information only) • Date of Birth • Service Provision Dates • Current care pathway 	<p>GDPR Go to articles 6 - 9</p>

- **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 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

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the Data Protection Act 1998 Conditions for Processing (Schedules 2 & 3) **ONLY VALID UNTIL 25TH MAY 2018***

Personal Data	Sensitive Personal Data
Sharing personal information in accordance with this protocol is lawful under the <i>Data Protection Act 1998</i> Schedule 2:	Sharing personal information in accordance with this protocol is lawful under the <i>Data Protection Act 1998</i> Schedule 3: (if appropriate): <i>[please complete]</i> :
2 (1) - Consent	3 (2) - Required by Law
2 (3) - Required by Law	Choose an item.
2 (5) - Administration of Justice/Public Functions	Choose an item.
Choose an item.	Choose an item.

Other legislation or statute as follows [

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

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the **General Data Protection Regulation 2016 (GDPR)**).*

GDPR
Go to articles
6-14

Personal Data	Special Categories of Data			
Sharing personal information in accordance with this protocol is lawful under the <i>General Data Protection Regulation 2016</i> article 6:	Sharing personal information in accordance with this protocol is lawful under the <i>General Data Protection Regulation 2016</i> article 9: (if appropriate): <i>[please complete]</i> :			
<i>Consent</i>	Explicit Consent			
<i>Legal Obligation</i>	Health & Social Care			
<i>Public Task</i>	Choose an item.			
Fair Processing in accordance with <i>General Data Protection Regulation 2016</i> article 12.				
Fair processing requirements have been satisfied by each organisation providing a privacy notice at the point of data collection.				
4.		Responsibilities		
For the purposes of this Protocol the responsibilities are defined as:	√ or ×	Organisation Name(s)	GDPR Go to articles 13-14, 24 - 31	
The Joint Data Controllers for this sharing are: <i>Where two or more controllers jointly determine the purposes and means of processing, they will be joint controllers. They will in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular with regard to the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by an arrangement between them unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects</i>	√	All Partners listed as party to this protocol on page 1.		
In the case of Joint Data Controllers , the designated contact point for Data Subjects is: <i>This is to provide a single point of contact for Data Subjects</i>		North East London Foundation Trust		
This Protocol will be reviewed one year after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by Essex County Council				

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?	X
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	√

Personal information will be securely shared via **PSN email nhs.net to GCSx** or Egress secure email system

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 of the information shared is as necessary for the particular activity, but generally will be in electronic text report form.

The frequency with which the information will be shared is as and when the need arises.

8.	Data Retention
-----------	-----------------------

GDPR

	Information will be retained in accordance with each partners' published data retention policy and in any event no longer than is necessary.	Go to article 5
9.	Data Accuracy	
	The primary responsibility for quality assurance checks sits with NELFT who manage the operational data on a day to day basis. They will apply their standard organisational procedures to manage data accuracy	GDPR Go to articles 5, 16 - 18
10.	Breach Notification	
	<p>Where a security breach linked to the sharing of data under this protocol is likely to adversely affect a data subject, Partners are required to inform all involved Partners 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.</p> <p>All involved Partners should consult on the need to inform the Data Subject, 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.</p> <p>All Partners to this protocol 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.</p> <p>A processor is liable for any damage caused by processing, only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.</p>	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 an attached email of approval from the signatory. The Protocol will then be published on weisf.essex.gov.uk.