

WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET



Title of Agreement: Essex Substance Misuse Caseload Management System

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Cyber Media Solutions Ltd (Theseus)	Opus House Priestly Court Staffordshire Technology Park Stafford St18 0Lq	01785 222350	Roland.corbet@cyber-media.co.uk	Roland Corbet	Z6767618
Essex County Council	County Hall Market Road Chelmsford Essex CM1 1QH	08457 430430	informationgovernanceteam@essex.gov.uk dpo@essex.gov.uk	Paul Turner	Z6034810
Essex Partnership University NHS Foundation Trust (Essex STaRS)	Trust Head Office The Lodge Lodge Approach Runwell Wickford SS11 7XX	01268 407737	alice.williams16@nhs.net	Alice Williams	ZA242481
Forward Trust	Unit 106-107 Edinburgh House 170 Kennington Land London SE11 5DP	020 3981 5525	lorna.cox@forwardtrust.org.uk	Lorna Cox	Z7310452
Open Road (Choices)	12 North Hill Colchester Essex CO1 1DZ	01206 369782	joni.thompson@openroad.org.uk	Joni Thompson	Z509709X
Phoenix Futures (Futures in Mind, Full Circle and PAIRS)	68 Newington Causeway London SE1 6DF	020 7234 9740	ali.saka@phoenix-futures.org.uk	Ali Saka	Z5753869
The Children's Society (Choices)	Edward Rudolf House Margery Street	0207 8414400	ian.wakeling@childrenssociety.org.uk	Ian Wakeling	Z9480097 and Z8912805

	London WC1X 0JL				
Peabody	45 Westminster Bridge Rd London SE1 7JB	01206 773005	Debbie.stephenson@peabody.org.uk	Debbie Stephenson	Z5696189

Version Control

Date Agreement comes into force	1 st April 2023
Date of Agreement review	1 st April 2026
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Shaun Cook- Senior Analyst
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	1.0

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
------	----------------------	-----------------------

Data Protection Impact Assessment (DPIA)	Theseus Project-1332	Essex County Council
Supporting Standard Operating Procedure		
Associated contract	Contracts completed with each provider	
Associated Policy Documents		
Other associated supporting documentation		

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

1 – Purpose

Essex Drug and Alcohol Treatment and Recovery System (EDATRS) is a group of agencies and organisations commissioned by Essex County Council working in partnership to deliver substance misuse treatment and provide recovery support to Essex residents should they need it.

The purpose of this protocol is to outline the legal terms and conditions which apply to the management and sharing of personal information by all EDATRS partners. Within this protocol information sharing refers to two or more providers or organisations sharing information between them.

The secure and appropriate transfer of confidential information is a vital part of an effective treatment and recovery system. It is essential to;

Monitor how effective drug and alcohol treatment services are (this helps ensure equitable funding of drug and alcohol treatment services nationally).

- Support and evaluate the improvement of outcomes for service users
- Help plan and develop services that best meet local needs
- Produce Statistics and support research to inform policy decisions
- Monitor the effectiveness of the government drug and alcohol strategies
- Promote partnership working
- Joint planning
- An integrated treatment response

It is therefore vital that all EDATRS partners demonstrate a commitment to share information responsibly, appropriately and securely. They must establish open, transparent and accountable procedures and agreements that manage the exchange of information to aid service delivery whilst keeping personal information protected throughout.

Providers signing up to this protocol also agree to adhere to the principles for information-sharing between drug and alcohol treatment services (the data providers) and Office for Health Improvement & Disparities' (OHID) National Drug and alcohol Treatment Monitoring System (NDTMS). This embedded Data Sharing Protocol sets out the conditions that all people working for or with the data providers must follow when sharing information with OHID and how OHID will hold and use that data securely and as declared.

[NDTMS: privacy notice - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/consultations/ndtms-privacy-notice)



NDTMS_Data_Sharing_Protocol_2018.pdf

2 – Information to be shared

The information to be shared is:

Personal data:

Each commissioned provider will collect data in order to provide each service. The data is likely to be:

- Forename, Surname, Date of Birth, Gender and Title
- Address, Phone Number, Email Address

Special categories of personal data:

- Ethnicity, Nationality, Religion, Sexuality
- Disability
- Personal history
- Social circumstances
- Physical and mental health information
- Prescribing information
- Safeguarding information
- Disclosed criminal activity
- Identified risks and/or vulnerabilities
- Previous treatment

The privacy notice for this data is here titled 'How we use your information':



EDAP%20Privacy%20
Notice.docx

The data collected by NDTMS is partially identifying information including initials, date of birth, sex, the local authority area in which service users live and the first part of their postcode. The data items and potential responses are declared in the NDTMS reference data document which can be found at: [NDTMS Reference Data CDSQ & NDTMS CJIT reference data CDSQ](#)

Other forms for use

[NDTMS: privacy notice - GOV.UK \(www.gov.uk\)](#)

[NDTMS: information and consent \(accessible version\) - GOV.UK \(www.gov.uk\)](#)



EARS Consent to
Share Information Au

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: <i>[please click Choose an item and select]</i>	Article 9: (if appropriate): <i>[please click Choose an item and select]</i>	DPA Part 3 (if appropriate): <i>[please click Choose an item and select]</i>
Public Task	Substantial Public Interest	Choose an item.
Legal Obligation	Health & Social Care	Choose an item.
Choose an item.	Choose an item.	Choose an item.
Choose an item.	Choose an item.	Choose an item.

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

Health and Social Care Act 2012 - Section 12 'Duties as to improvement of public health'

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
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 checked="" type="checkbox"/>	Cyber Media Solutions Ltd; Essex County Council; Essex Partnership University NHS Foundation Trust; Forward Trust; Mid and North Essex Mind; Mind in West Essex; Open Road; Peabody; Phoenix Futures; The Children's Society

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>	<p>N/A</p>
<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</p>	<input checked="" type="checkbox"/>

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

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.

This information will be stored within the Theseus System so not data will be transferred between any organisations.

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 & Frequency

- The format the information will be shared in is **web-based caseload management system**
- The frequency with which the information will be shared is **Live access**

If a shared system is being used by partners:

- What system is being shared? **Theseus**

- Who is the owner of the system? **Cyber Media Solutions Ltd**

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>