

WEISF INFORMATION SHARING PROTOCOL

SUMMARY SHEET



Title of Agreement: Rough Sleepers Covid Vaccination Programme

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, CM1 1QH	08457 430430	IGTeam@essex.gov.uk	Paul Turner	Z6034810
Southend on Sea Borough Council	Civic Centre, Victoria Avenue, Southend on Sea, Essex, SS2 6ER	01702 215 000	Dataprotection@southend.gov.uk	Valerie Smith	Z6929331
Thurrock Borough Council	PO BOX 1 CIVIC OFFICES NEW ROAD GRAYS THURROCK ESSEX RM17 6SL	01375 652000	Information.matters@thurrock.gov.uk	Lee Henley	Z8228055
Essex Partnership NHS University Foundation Trust	The Lodge Lodge Approach Runwell Wickford SS11 7XX	01268 407737	Epunft.info.gov@nhs.net	Claire Sladden	ZA242481
Hertfordshire Community NHS Trust	Unit 1A Howard Court, 14 Tewin Road, Welwyn Garden City, Herts, AL7 1BW	01707 388000	Hct.atr@nhs.net	Martin Vitty	Z2489526

Version Control

Date Agreement comes into force	March 2021
Date of Agreement review	March 2022
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	ECC Information Governance and Housing Growth Team
Status of document – DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	V1.3

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)	1107	ECC
Supporting Standard Operating Procedure	NA	
Associated contract	NA	
Associated Policy Documents	NA	
Other associated supporting documentation	N/A	

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

1 – Purpose

This Information Sharing Protocol sets out the overarching Information Sharing Principles between Essex County Council (ECC), (the 12 Districts), Southend BC, Thurrock BC, Essex Partnership University NHS Foundation Trust (EPUT) and Hertfordshire Community NHS Trusts in sharing data between the organisations. ECC has all the data from the Local Authorities which will be shared/held within a spreadsheet and will be sharing this with EPUT/Hertfordshire Community NHS Trust.

Effectively sharing information relating to rough sleepers within Essex to establish whether they have been offered and if they so wish been provided with their Covid-19 vaccination through the sharing of their details.

We wish to share with health colleague's information on approx. 650 rough sleepers specifically for the Covid vaccination programme for this marginalised and vulnerable group. This information will be provided by ECC, Southend and Thurrock under Covid Legislation.

Data sharing will enable the Council to fulfil key strategic responsibilities, including:

- ensuring that the vaccination programme reaches some of the most vulnerable in society;
- support EPUT in providing the vaccine to those individuals who have been identified as not having been offered or received a vaccination;
- ensuring effective planning, commissioning, and delivery of services to rough sleepers;
- The information provided to health would be used solely for the use in the Rough Sleeper Covid vaccination programme and allow us to pass information to health on who they need to offer a vaccination too. We would like data back from health on who has and hasn't had their vaccination, for the sole purpose of maximising the numbers of rough sleepers who get their first and 2nd vaccines.

No information would be held or stored by any of the parties for any other reason or for a time period outside this vaccination programme.

2 – Information to be shared

Arrangements for information sharing relating to planning and provision of vaccinations for Covid-19 to rough sleepers within Essex. This agreement specifies the data relating to individual rough sleepers that will be shared and which will be identified which individuals have had their vaccination and which have not. This will include:

- Name & Date of Birth
- District of Residence (Local Authority/Area)
- Vaccination status

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: (if appropriate):	DPA Part 3 (if appropriate): <i>N/A</i>
<i>Legal Obligation</i>	Public Interest in Public Health	Choose an item.
<i>Public Task</i>	Health & Social Care	Choose an item.
Choose an item.	Choose an item.	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, [Covid-19 and our use of data during the pandemic - Essex County Council](#)

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

Coronavirus Act 2020
Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 - general
Care Act 2014
Health and Social Care Act 2012

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"/>	ECC, Southend BC, Thurrock BC, EPUT & Hertfordshire Community NHS Trust
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 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;">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>Processes are in place to enact this right - please check the box</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.	<input checked="" type="checkbox"/>
GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner	<input checked="" type="checkbox"/>
GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	<input checked="" type="checkbox"/>
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.	<input type="checkbox"/>
GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>

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.	<input type="checkbox"/>
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.	<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 the spreadsheet being sent via email and being password protected, which will be sent between ECC (.gov email address) and EPUT/Hertfordshire Community NHS Trust (.NHS.net email address). The password will be sent in a separate email from the spreadsheet. The LA's involved in this sharing will be able to share their information via normal email routes due to all having .gov email addresses and the security measures that these addresses have.

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 **an Excel spreadsheet**
- The frequency with which the information will be shared is **this will be over the next 12 months and in all likelihoods only for the next 3 months. We would expect that to pass over a list of approx. 650 rough sleeper names, dob and districts of residence to health teams probably only once a week and for health to pass back this information to ourselves as and when a rough sleeper has been vaccinated. This information will solely be used to maximise the vaccination program and will be destroyed at the end of the programme.**

If a shared system is being used by partners:

- What system is being shared? **N/A**
- Who is the owner of the system? **N/A**

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