

INFORMATION SHARING PROTOCOL

SUMMARY SHEET



Title of Agreement Adult Social Care Users and Carers Survey					
Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	Essex County Council, County Hall, Market Road, Chelmsford, Essex, CM11QH	0333 013 9824	DPO@essex.gov.uk	Paul Turner	Z6034810
NHS Digital		0300 303 5678	enquiries@nhsdigital.nhs.uk england.dpo@nhs.net	Carol Mitchell	Z8959110
QA Research	Merchant House, 11a Piccadilly, York, YO1 9WB	01904 632039	dpo@qaresearch.co.uk	Nancy Rhodes	Z8603006

Version Control	
Date Agreement comes into force	
Date of Agreement review	2022
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Alison Dellow – Information Governance/Neave Beard - Researcher
Status of document – DRAFT/FOR APPROVAL/APPROVED	For Approval
Version	V0.1

Wider Essex 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
DPIA	809	Essex County Council
Supporting Standard Operating Procedure		
Associated contract	Contract with QA (number to follow)	
Associated Policy Documents		
Other associated supporting documentation		

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

1.	Purpose	REFERENCES
	<p>PLEASE EXPLAIN THE REASON YOU WISH TO SHARE DATA HERE</p> <p><i>The National Health Service has a duty to improve services under the Health and Social Care Act 2012, which Essex County Council are obligated (as a local authority) to assist with under the National Health Service Act 2006.</i></p> <p>This is undertaken through the completion of two annual surveys which are shared with NHS digital. https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/social-care-user-surveys</p> <p><i>The National Health Service uses this information for the purposes of completing the Adult Social Care Outcomes Toolkit (ASCOT) measures. The adult social care survey asks people who are over 18 and who use adult social care about their experiences. NHS Digital run this every year and it looks at how these services are helping people to live safely and independently in their own homes. ASCOT is designed to capture information about an individual's social care-related quality of life.</i></p> <p><i>In addition Essex County Council has a duty to the public to improve social services under the Care Act 2014, therefore these survey results are used to aid service improvement.</i></p>	<p>GDPR Go to article 5</p>
2.	Information to be shared	

Agency Name	Data field/description
Essex County Council (being shared with NHS who will receive the final coded data)	<ul style="list-style-type: none"> • Name & address
	<ul style="list-style-type: none"> • Age band
	<ul style="list-style-type: none"> • Gender
	<ul style="list-style-type: none"> • Ethnicity
	<ul style="list-style-type: none"> • Religion
	<ul style="list-style-type: none"> • Method of assessment or review
	<ul style="list-style-type: none"> • Support provided to carer
	<ul style="list-style-type: none"> • Support involving the cared-for person
	<ul style="list-style-type: none"> • Funding status (cared-for person)
	<ul style="list-style-type: none"> • Delivery mechanism of long-term support for the cared-for person
	<ul style="list-style-type: none"> • Primary support reason of the cared-for person
Agency Name	Data field/description
QA Research	QA Research will provide NHS Digital with the following:
	<ul style="list-style-type: none"> • Method of collection
	<ul style="list-style-type: none"> • Whether carer has responded or not
	<ul style="list-style-type: none"> • Age band
	<ul style="list-style-type: none"> • Gender
	<ul style="list-style-type: none"> • Ethnicity
	<ul style="list-style-type: none"> • Religion
	<ul style="list-style-type: none"> • Method of assessment or review
	<ul style="list-style-type: none"> • Support provided to carer
	<ul style="list-style-type: none"> • Support involving the cared-for person
	<ul style="list-style-type: none"> • Funding status (cared-for person)
	<ul style="list-style-type: none"> • Delivery mechanism of long-term support for the cared-for person
	<ul style="list-style-type: none"> • Primary support reason for the cared for person
	<ul style="list-style-type: none"> • Reported health condition of the cared-for person

GDPR
Go to articles 6
- 9

	<ul style="list-style-type: none"> • Whether an advocate has been used 	
	<ul style="list-style-type: none"> • Whether they needed an interpreter 	
	<ul style="list-style-type: none"> • Whether a translated version was used 	
	<ul style="list-style-type: none"> • Whether a carer responded to original postal questionnaire or a reminder 	

3.	Legal Basis	
-----------	--------------------	--

General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.

GDPR
Go to articles 6-14

Personal Data (identifiable data)	Special Categories of Data (Sensitive identifiable data)
Article 6: <i>[please click and select]</i>	Article 9: (if appropriate): <i>[please click and select]</i>
<i>Legal Obligation</i>	Health & Social Care
<i>Public Task</i>	Choose an item.

Other legislation or statute as follows:
Health and Social Care Act 2012.
National Health Service Act 2006.
Care Act 2014.

4.	Responsibilities	
-----------	-------------------------	--

For the purposes of this Protocol the responsibilities are defined as follows:	Tick box	Organisation Name(s)
--	----------	----------------------

GDPR
Go to articles 13-14, 24 - 31

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.			
The Sole Data Controller for this sharing is:	<input type="checkbox"/>		
The Joint Data Controllers for this sharing are:	<input checked="" type="checkbox"/>	<i>Essex County Council</i> <i>NHS Digital</i>	
In the case of Joint Data Controllers , the designated single contact point for Individuals is: Katerina Glover, Essex County Council	<input checked="" type="checkbox"/>	Essex County Council	
Data Processors party to this protocol are (please list): QA Research	<input checked="" type="checkbox"/>		
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 Alastair Gordon			
5.	Subject Rights		
Essex Partner Agencies' Information Sharing Agreements are made publicly available on the Whole Essex Information Sharing Framework 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.		<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 Go to article 16 & 22
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 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 restrict, 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.	<input checked="" 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		GDPR articles 30 - 45
Security measures in place		
There are good quality access control systems in place	<input checked="" type="checkbox"/>	
Paper information is stored securely	<input checked="" type="checkbox"/>	
Paper and electronic information is securely destroyed with destruction log for electronic information	<input checked="" type="checkbox"/>	

Laptops and removable media such as memory sticks are secured when not in use	<input checked="" type="checkbox"/>
Technical security appropriate to the type of information being processed is applied	<input checked="" type="checkbox"/>
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	<input checked="" type="checkbox"/>
Disaster recovery arrangements are in place	<input checked="" type="checkbox"/>
Encryption of personal data is fully implemented	<input checked="" type="checkbox"/>
Data minimisation has been considered	<input checked="" type="checkbox"/>
Can pseudonymised or anonymised data be used to meet your processing needs?	<input checked="" type="checkbox"/>
There are sufficient access controls for systems/networks in place	<input checked="" type="checkbox"/>
Routine and regular penetration tests are carried out	<input checked="" type="checkbox"/>
Article 40 Codes of Conduct are adhered to (where applicable)	<input type="checkbox"/>
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	<input checked="" type="checkbox"/>
Confirm entry in Records of Processing Activity	<input checked="" type="checkbox"/>
Additional measure 1 – please specify here	<input type="checkbox"/>
Additional measure 2 – please specify here	<input type="checkbox"/>

Personal information will be shared 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	
<p>The format the information will be shared in is via a secure email, which will be shared with QA Research. QA Research will submit anonymised administrative data and question responses for everyone in the sample via a data sheet.</p> <p>The frequency with which the information will be shared is Annually</p>		
8.	Data Retention	
<p>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.</p>		<p>GDPR Go to article 5</p>
9.	Data Accuracy	
<p>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 <input checked="" type="checkbox"/></p>		<p>GDPR Go to articles 5, 16 - 18</p>
10.	Breach Notification	
<p>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.</p> <p>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.</p>		

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.	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