INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	COVID-19 Contact Tracing – Environmental Health Officers

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, CM1 1QH	08457 430430	Informationgovernanceteam@essex.gov.uk	Paul Turner	Z6034810
Basildon Borough Council	The Basildon Centre, St Martins Square, Basildon, Essex, SS14 1DL		Sue.marriott@basildon.gov.uk	Sue Marriott	Z5361180
Braintree District Council	Causeway House, Bocking End, Braintree, Essex, CM7 9HB	01376 552525	DPO@braintree.gov.uk	Kim Cole	Z5103738
Brentwood Borough Council	Town Hall, Ingrave Road, Brentwood, Essex, CM15 8AY	01277 312500	Amanda.julian@brentwood.gov.uk	Amanda Julian	Z2092695

Castle Point Borough Council	Council Offices, Kiln Road, Benfleet, Essex, SS7 1TF		legal@castlepoint.gov.uk	Andrew Roby Smith	Z588703X
Chelmsford City Council	Civic Centre, Duke Street, Chelmsford, Essex, CM1 1JE		John.breen@chelmsfordcc.gov.uk ir@chelmsford.gov.uk	John Breen	Z7829039
Epping Forest District Council	Civic Offices, High Street, Epping, Essex, CM16 4BZ		dataprotection@eppingforestdc.gov.uk		Z5033101
Harlow District Council	Civic Centre, The Water Gardens, College Square, Harlow, Essex, CM20 1WG		data.protection@harlow.gov.uk		Z7603332
Maldon District Council	Princes Road, Maldon, Essex, CM9 5DL	01621 876224	dpo@maldon.gov.uk	Emma Holmes	Z6616948
Rochford District Council	Council Offices, South Street, Rochford, Essex, SS4 1BW		dpo@rochford.gov.uk	Angela Law	Z6617133
Southend-on-Sea Council	Civic Centre Victoria Avenue Southend-On-Sea Essex SS2 6ER	01702 215000	dataprotection@southend.gov.uk	Valerie Smith	Z6929331

Tendring District Council	Town Hall, Station Road, Clacton On Sea, Essex, CO15 1SE	01255 686060	DPAOfficer@tendringdc.gov.uk	Judy Barker	Z577148X
Uttlesford District Council	London Road, Saffron Walden, Essex, CB11 4ER	01799 510510	dpo@uttlesford.gov.uk		Z5060641

Version Control	
Date Agreement comes into force	July 2020
Date of Agreement review	July 2021
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Gemma Gibbs, Senior Information Governance Officer, ECC
Status of document – DRAFT/FOR APPROVAL/APPROVED	FOR APPROVAL
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
Privacy Impact Assessment (PIA/DPIA)		
Supporting Standard Operating Procedure		
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the WEISF Portal.

1.	Purpose	REFERENCES
As part of the National response to the COVID-19 pandemic, Public Health England set up the Test and Trace service in May 2020. Local authorities have been identified to provide support for complex cases by setting up contact tracing services. The Essex County Council and Southend Contact Tracing Service (Hub) will co-ordinate the local Covid-19 contact tracing response process in line with government guidelines. The service will cover all geographical areas in Essex including the unitary authority area of Southend-on-Sea but excluding the unitary authority area of Thurrock. The service will be directly engaging with the twelve local city/borough/district councils in Essex as well as other partner agencies (e.g. Open Road, Peabody and Phoenix Futures). When Environmental Health Officers (EHOs) help is needed for a setting/locality the Case will be assigned to them by the Hub. EHO actions: • contacting local businesses/workplaces identified by a Case • carrying out a risk assessment/inspection • providing advice to the organisation/establishment on their operational procedures in light of the pandemic • identify potential Contacts so that they can be advised on what they need to do It is likely that the EHO will need to have personal identifiable information to aid the accuracy of their investigation and assistance in identifying potential Contacts (those who may have come into close contact with the person who has tested positive for Covid-19). The EHO will be able to provide the Employer with template letters that can be issued to staff with advice on self-isolating where it is necessary and what action to take if they become symptomatic. There may be occasions where the EHO will be the Notifier and will provide the information to the Hub (via the Case Management System or appropriate secure method) where it will be assigned. It could in effect be assigned back to the same EHO team to follow up.	GDPR Go to article 5

2. Information to be shared

GDPR
Go to articles 6 - 9

The case management system will capture the information detailed below. This will be accessible to view by the EHOs but there is an expectation that they will use their professional judgement to ascertain the necessary information required to carry out their function. When dealing with a setting/establishment they will need to minimise the information that is disclosed to what is necessary. It may be necessary to disclose the name of the person who has a positive Covid-19 test to establish the potential contacts as per the contact tracing process.

- Unique Record ID
- Full name
- Date of birth
- Gender
- Ethnicity
- Home postcode
- Telephone number and email address
- Occupation/key worker type
- COVID-19 symptoms, including when they started and their nature
- Vulnerability Group
- Shielded Status
- Locality
- Setting Type (which may be their place of work)
- Setting Contact

3. Legal Basis

GDPR
Go to articles 6-14

General Data Protection Regulation 2016 (GDPR) and 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**:	**DPA Part 3** (if appropriate): Not Applicable
Public Task	Public Interest in Public Health	Choose an item.

Other legislation or statute as follows:
COVID-19 Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002

4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

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:	☒	All signatories
The Joint Data Controllers for this sharing are:	☐	
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☐	
Data Processors party to this protocol are (please list):	☒	Provide and their subcontractors

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.

5. Subject Rights

Essex 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.

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 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.	☒	GDPR Go to articles 12 – 15
GDPR Article 15 – **Right of Access** – Individuals have the right to request access to the information about them held by each Partner	☒	
GDPR Article 16 – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	☒	
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.	☐	
GDPR Article 18 – **Right to Restriction** – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☒	
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.	☒	GDPR Go to article 16 & 22
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.	☒	
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.	☐	
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.		

6. Security of Information

Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
Paper information is stored securely	☒	
Paper and electronic information is securely destroyed with destruction log for electronic information	☒	
Laptops and removable media such as memory sticks are secured when not in use	☒	
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?	☐	
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	☒	
Confirm entry in Records of Processing Activity	☐	
Any risks associated with this data sharing have been assessed by your organisation and approval to proceed granted by your authorising signatories	☒	
Additional measure 1 – please specify here	☐	
Additional measure 2 – please specify here	☐	

Personal information will be securely shared via secure email or Case Management 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
- Only access the information required to complete their specific task. It must be proportionate to the activity.
- Not carry out unauthorised searches of the Essex County Council and Southend Contact Tracing Case Management System

7. Format and Frequency

- The format the information will be shared in is CSV file from PHE. The Case Management System will be used by partners to access the incidents, cases and contacts where appropriate. Secure email will be used where it is necessary.
- The frequency with which the information will be shared as necessary on a case by case basis. This will be determined during the triage process.

If a shared system is being used by partners:

- What system is being shared? Microsoft Dynamics System
- Who is the owner of the system? Essex County Council

8. Data Retention

Information will be retained in accordance with the COPI Notice received by the Department of Health and Social Care. Initial destruction date of 30 September 2020 with an expectation that it will be extended. It is the responsibility of Data Controllers to ensure that they destroy the data in line with the COPI Notice and keep up to date with any review. Data Processors must comply with contractual arrangements detailing the destruction and notifying procedure.

GDPR
Go to article 5

COPI Notice Links https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/874509/Coronavirus__COVID-19____notice_under_regulation_3_4__of_the_Health_Service_Control_of_Patient_Information_Regulations_2002.pdf		
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 ☒		GDPR Go to articles 5, 16 - 18
10.	**Breach Notification**	
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.		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	*John Higgins* John Higgins, Head of IT & Resilience (SIRO)
Organisation Name	Tendring District Council
Date of Agreement	23/11/20

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