

# INFORMATION SHARING PROTOCOL

## SUMMARY SHEET



<b>Title of Agreement</b> BEST/BES/K&M Growth Hub Data Sharing Protocol to support the Local Enterprise Partnership					
<b>Organisation Name</b>	<b>Head Office Address</b>	<b>Phone</b>	<b>Email</b>	<b>Named Data Protection Officer</b>	<b>ICO Notification reference</b>
Southend on Sea Borough Council	Civic Centre, Victoria Avenue, Southend, SS2 6EX	01702 417765	bestgrowthhub@southend.gov.uk	Debee Skinner	Z6929331
Kent County Council	Sessions House, County Road, Maidstone, Kent, ME14 1XQ	03000416814	dpo@kent.gov.uk	Benjamin Watts	Z5297748
Medway Council	Gun Wharf, Dock Road, Chatham, Kent, ME4 4TR	01634 334329	gdpr@medway.gov.uk	Gayle Jones	Z5895541
East Sussex County Council	East Sussex County Council, County Hall, St Anne's Crescent, Lewes, East Sussex BN7 1UE	0345 608 0190			Z5664005
Essex County Council	County Hall, Chelmsford. CM1 1QH	03330132984	DPO@essex.gov.uk	Paul Turner	Z6034810
<b>Version Control</b>					
<b>Date Agreement comes into force</b>			30 <sup>th</sup> November 2018		
<b>Date of Agreement review</b>			1 year after signing		
<b>Agreement owner (Organisation)</b>			Essex County Council		
<b>Agreement drawn up by (Author(s))</b>			Lauri Almond		
<b>Status of document – DRAFT/FOR APPROVAL/APPROVED</b>			For approval		

<b>Version</b>	1
----------------	---

# 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		Southend Borough Council East Sussex County Council
Supporting Standard Operating Procedure	N/A	N/A
Associated contract	Grant Agreement	Essex County Council
Other associated supporting documentation	N/A	N/A

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

1.	Purpose	REFERENCES
	<p>The information is being shared:</p> <ul style="list-style-type: none"> <li>i. to facilitate the delivery and management of business support services to SMEs in the East Sussex, Essex, Kent, Medway, Southend and Thurrock area provided by South East Local Enterprise Partnership (SELEP) under the auspices of the BEST, BES and K&amp;M Growth Hubs; supported by delivery partners Let's do Business (BES) and Kent Invicta Chamber of Commerce (K&amp;M)</li> <li>ii. to report effectively on the performance of the BEST/BES/K&amp;M Growth Hubs to the funding body, the Department for Business, Energy and Industrial Strategy (BEIS)</li> <li>iii. to enable SELEP to report key metrics back to BEIS in relation to evaluating customer satisfaction and demonstrating value for money of the service</li> <li>iv. to enable SELEP to report business data to the funders, BEIS as set out in the offer letter as a requirement of the funding awarded to deliver the service</li> <li>v. to enable SELEP any contractors working on behalf of SELEP to undertake statistical analysis and/or compile reports of the business support services provided by the BEST/BES/K&amp;M Growth Hubs and its other delivery partners</li> <li>vi. to allow BEST/BES/K&amp;M Growth Hubs to track the progress of specific SMEs who have received business support services</li> </ul>	<p>GDPR Go to article 5</p>
2.	Information to be shared	
	<p>The information that may be shared between the parties:</p> <ul style="list-style-type: none"> <li>i. contact name and address details including post code and local authority located in (both individuals and businesses)</li> <li>ii. contact details including phone numbers and emails (both individuals and businesses)</li> <li>iii. business name, business registration date, legal status and ownership details</li> <li>iv. description of the business, maturity of the business, sector and SIC code</li> </ul>	<p>GDPR Go to articles 6 - 9</p>

v.	website address
vi.	reason for contacting the Growth Hub, how they heard about the Growth Hub / source of referral
vii.	companies house number, VAT registration number, HMRC unique taxpayer reference (UTR), HMRC employers PAYE reference number
viii.	evidence of its eligibility as an SME to receive support, including turnover and number of employees
ix.	length of interaction
x.	narrative details of each instance of support provided by SELEP under the auspices of the BEST/BES/K&M Growth Hub, including but not limited to details of the support the SME is seeking, the business objectives, the area of growth identified, the barriers to growth, the cost to the business, the support received, the outcome of that support (could be jobs created / safeguarded, increase in turnover etc.) and details of who the business was referred to and the details of that referral, including the outcome of that referral
xi.	Satisfaction rating with the Growth Hub service

<b>3.</b>	<b>Legal Basis</b>
-----------	--------------------

<p>As a funded service, we have a legitimate interest for sharing business data with our funders, the Department for Business, Energy and Industrial Strategy (BEIS) as it is a requirement of our funding that we report to BEIS the details of individuals / businesses that we have supported for statistical analysis and evaluation purposes. It is the choice of the business to use the business support service that we are providing.</p>		<p>GDPR Go to articles 6-14</p>
<b>Personal Data</b>	<b>Special Categories of Data – NOT APPLICABLE</b>	
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>Legitimate Interests</i>	Choose an item.	
<i>Consent</i>	Choose an item.	
<i>Under Contract</i>	Choose an item.	

Public Task

Choose an item.

Other legislation or statute as follows  
Local Government Act 1972  
Localism Act 2011

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12 is satisfied by:

The businesses that have provided their information in order to take up the BEST/BES/K&M Growth Hub service have been advised on the diagnostic form under the declaration section what their data will be used for and have been given the opportunity to consent to further sharing of information that is not compulsory. The Best/BES/K&M Growth Hubs also have a privacy notice available on their website with more information related to the use of their data.

**4. Responsibilities**

For the purposes of this Protocol the responsibilities are defined as:	√ or ×	Organisation Name(s)
The sole Data Controller for this sharing is		
The Joint Data Controllers for this sharing are:	√	All partners party to this protocol
In the case of <b>Joint Data Controllers</b> , the designated contact point for Data Subjects is:	√	Essex County Council
Data Processors party to this protocol are:	√	Let's Do Business Group (East Sussex) and Kent Invicta Chamber of Commerce (Kent & Medway)

This Protocol will be reviewed three years after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by Essex County Council.

GDPR  
Go to articles  
13-14, 24 - 31

5.	Subject Rights									
<p>GDPR Article 15 - <b>Subject Access</b> - is an individual's right to have a copy of information relating to them which is processed by an organisation.</p> <p>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> <p>Once information is disclosed from one agency to another, the recipient organisation becomes the <b>Data Controller</b> for that information. With regards to subject access requests, the <b>Data Controller</b> has a statutory duty to comply with article 15 of the GDPR, unless derogation applies. It is good practice for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory derogation that may need to be applied prior to disclosure to the requesting individual. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory one month (additional two months for complex SARs), time period.</p> <p>If a party receives a request for information under the <b>Freedom of Information (FOI) Act 2000</b> or <b>Environmental Information Regulations (EIR) 2004</b> that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, 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 under the provisions of the FOI Act or EIR 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.</p> <p>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.</p> <p>GDPR Article 17 (1)(b)&amp;(e) – <b>Right to be forgotten</b> – This right may apply where the sharing is based on consent, 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 to ensure compliance with the GDPR.</p>		<p>GDPR Go to articles 12 – 22</p> <p>GDPR Go to article 17 &amp; 19</p>								
6.	Security of Information									
	<table border="1"> <thead> <tr> <th data-bbox="463 1294 1626 1339">Control in place</th> <th data-bbox="1626 1294 1850 1339">√ / x</th> </tr> </thead> <tbody> <tr> <td data-bbox="463 1339 1626 1375">There are good quality access control systems in place</td> <td data-bbox="1626 1339 1850 1375">Yes</td> </tr> <tr> <td data-bbox="463 1375 1626 1412">Paper information is stored securely</td> <td data-bbox="1626 1375 1850 1412">Yes</td> </tr> <tr> <td data-bbox="463 1412 1626 1444">Paper and electronic information is securely destroyed with destruction log for electronic information</td> <td data-bbox="1626 1412 1850 1444">Yes</td> </tr> </tbody> </table>	Control in place	√ / x	There are good quality access control systems in place	Yes	Paper information is stored securely	Yes	Paper and electronic information is securely destroyed with destruction log for electronic information	Yes	<p>GDPR articles 30 - 45</p>
Control in place	√ / x									
There are good quality access control systems in place	Yes									
Paper information is stored securely	Yes									
Paper and electronic information is securely destroyed with destruction log for electronic information	Yes									

Laptops and removable media such as memory sticks are secured when not in use	Yes
Technical security appropriate to the type of information being processed is applied	Yes
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	Yes
Disaster recovery arrangements are in place	Yes
Encryption of personal data is fully implemented	Yes
Data minimisation has been considered	Yes
Can pseudonymised or anonymised data be used to meet your processing needs?	No
There are sufficient access controls for systems/networks in place	Yes
Routine and regular penetration tests are carried out	Yes
Article 40 Codes of Conduct are adhered to (where applicable)	Yes
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	Yes

The information is shared via a CRM system which has 2 factor authentication.

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 3<sup>rd</sup> party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

<b>7.</b>	<b>Format and Frequency</b>
-----------	-----------------------------

Data is shared by input to the CRM. The data will be accessed and used to provide the requested support where possible.

The frequency with which the information will be shared is daily via the CRM.

<b>8.</b>	<b>Data Retention</b>
-----------	-----------------------

Information will be retained for 6 years in accordance with the monitoring and evaluation framework provided by

GDPR  
Go to article 5



BEST/BES/K&M Growth Hubs funders, The Department for Business, Energy and Industrial Strategy.		
<b>9.</b>	<b>Data Accuracy</b>	
Data will be kept up to date through ongoing engagement with the businesses and individuals and any changes to the data will be made on the CRM system within a suitable timeframe of being informed (10 working days).		GDPR Go to articles 5, 16 - 18
<b>10.</b>	<b>Breach Notification</b>	
<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 immediately when the breach is 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
<b>11.</b>	<b>Complaints</b>	
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
<b>12.</b>	<b>Commencement of Protocol</b>	

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](mailto: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](mailto:weisf@essex.gov.uk) with an attached email of approval from the signatory. The Protocol will then be published on [weisf.essex.gov.uk](http://weisf.essex.gov.uk).**