INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	BEST Growth Hub Data Sharing Protocol

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Southend on Sea Borough Council	Civic Centre, Victoria Avenue, Southend, SS2 6EX	01702 417765	bestgrowthhub@southend.gov.uk	Debee Skinner	Z6929331
Tendring District Council	Tendring District Council Town Hall Station Road Clacton on Sea Essex CO15 1SE	01255 686060	DPAOfficer@tendringdc.gov.uk	Judy Barker	Z577148X

Version Control	
Date Agreement comes into force	31st May 2018
Date of Agreement review	1 year after signing
Agreement owner (Organisation)	Southend On Sea Borough Council
Agreement drawn up by (Author(s))	Georgia Searle
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	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	completed	Southend Borough Council
Supporting Standard Operating Procedure		
Associated contract		
Other associated supporting documentation		

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

1.	Purpose	REFERENCES
		GDPR Go to article 5

The information is being shared:

i. to facilitate the delivery and management of business support services to SMEs in the Essex, Southend and Thurrock area provided by South East Local Enterprise Partnership under the auspices of the BEST Growth Hub, supported by the Delivery Partner,

ii. to report effectively on the performance of the BEST Growth Hub to the funding body, the Department for Business, Energy and Industrial strategy (BEIS)

iii. to enable the South East Local Enterprise Partnership to report key metrics back to BEIS in relation to evaluating customer satisfaction of the scheme

iv. to enable the Delivery Partner to undertake statistical analysis and/or compile reports of the business support services provided by the BEST Growth Hub and its other delivery partners

v. to allow BEST Growth Hub to track the progress of specific SMEs who have received business support services

vi. to provide evidence that State Aid provided to the SMEs through the BEST Growth Hub is in accordance with European Community regulation 1998/2006

vii. to enable the Delivery Partner to contact SMEs who have received business support services from BEST Growth Hub. Any such contact with an SME by the Delivery Partner shall be solely for the purpose of:

- profiling business support activity in the relevant local authority area;
- contacting the SME to arrange face-to-face meetings;
- responding to a specific request made by an SME.

2.	Information to be shared	

The information to be shared between the parties: i. contact name and address details including post code and local authority located in (both individuals and businesses), position within the business ii. contact details including phone numbers and emails (both individuals and businesses) iii. business name, business registration date, legal status and ownership details iv. description of the business, maturity of the business, sector and SIC code 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 current and projected turnover and number of employees ix. State Aid provided to it during the last 3 (three) fiscal years x. data to demonstrate its Gross Value Added (i.e. annual sales, net profitability, depreciation costs, employment costs, tangible fixed assets and the number of employees) in the most recent, completed fiscal year and its own forecast for the current financial year xi. length of interaction xii. narrative details of each instance of support provided by South East Local Enterprise Partnership under the auspices of the BEST Growth Hub, including but not limited to details of the support the SME is seeking, the business objectives, the area of growth identified by navigators, 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. xiii. Satisfaction rating with the Growth Hub service	GDPR Go to articles 6 - 9

3. Legal Basis

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the **General Data Protection Regulation 2016** (GDPR)).*

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 business support service that we are providing.

We use consent when sharing data with Local Authorities as it is not a condition of the funding to share businesses/ individual's data with their Local Authority. We therefore seek opt-in consent from the individual / business before we share their details with their Local Authority. The sharing will take place to facilitate business support as outlined in Section 1 (Purpose) of this agreement.

Personal Data	**Special Categories of Data**
Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 6:	Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 9: (if appropriate): *[please complete]*:
Public Task	Choose an item.
Consent	Choose an item.
Under Contract	Choose an item.

Other legislation or statute as follows

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.

Fair processing requirements have been satisfied by:
The businesses that have provided their information in order to take up the BEST Growth Hub service have been advised on

GDPR
Go to articles 6-14

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 Growth Hub also have a privacy notice available on their website which more information related to the use of their data.

4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

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:	√	Tendring District Council and Southend On Sea Borough Council
In the case of **Joint Data Controllers**, the designated contact point for Data Subjects is:	√	Marta Koelner (martakoelner@southend.gov.uk) Southend On Sea Borough Council Judy Barker jbarker@tendringdc.gov.uk Tendring District Council
Data Processors party to this protocol are:	√	Tendring District Council and Southend On Sea Borough Council

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 Southend-On-Sea Borough Council

5. Subject Rights

GDPR
Go to articles 12 – 22

GDPR Article 15 - **Subject Access** - is an individual's right to have a copy of information relating to them which is processed by an organisation.

Once information is disclosed from one agency to another, the recipient organisation becomes the **Data Controller** for that information. With regards to subject access requests, the **Data Controller** 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 20 working days (additional 2 months for complex SARs), time period.

If a party receives a request for information under the **Freedom of Information** (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 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.

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.

GDPR Article 17 (1)(b)&(e) – **Right to be forgotten** – 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.

GDPR
Go to article 17 & 19

6. Security of Information

Control in place	√ / ×
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	Yes

GDPR
articles 30 - 45

remote access solutions	
Additional control 1 – please specify here	
Additional control 2 – please specify here	

Personal information will be securely shared via a password protected spreadsheet. In the future this may be shared via a CRM 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.

7. Format and Frequency

The format the information will be shared in is a password protected spreadsheet to be sent to a secure emails address that limited people have access to. In the future this may be shared via a CRM system.

The frequency with which the information will be shared is every two months via a password protected spreadsheet. If shared via a CRM system then the frequency could be daily as the joint data controller will have access to the CRM system.

8. Data Retention

Information will be retained for 6 years in accordance with the monitoring and evaluation framework provided by BEST Growth Hub's funders, The Department for Business, Energy and Industrial Strategy.

GDPR
Go to article 5

9. Data Accuracy

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
10.	**Breach Notification**	
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. 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. 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. 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.		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	
Organisation Name	Southend and Tendring Councils – Please contact the Lead Organisation for details of approvals
Date of Agreement	

Please submit this Protocol to weisf@essex.gov.uk with an attached email of approval from the signatory. The Protocol will then be published on weisf.essex.gov.uk.