WEISF

INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Transformation Challenge Award – Essex Data: Platform			
Organisation Name	**Head Office Address**	**Phone**	**Email**	**ICO Registration reference**
Essex County Council	County Hall. Chelmsford. Essex. CM1 1QH	08457 430430	Informationgovernanceteam@essex, gov.uk	Z6034810
Basildon Borough Council	The Basildon Centre. St Martins Square. Basildon. SS14 1DL.	01268 533333	Peter.Mckenzie@basildon.gov.uk	Z5361180
Essex Police	Essex Police Headquarters, PO Box 2, Springfield, Chelmsford, CM2 6DA	01245 491491	Andy.begent@essex.pnn.police.uk	Z4883472
University of Essex	Wivenhoe Park Colchester CO4 3SQ	01206 873333	r.skeggs@essex.ac.uk	Z699129X

Version Control	
Date Agreement comes into force	30/11/2016
Date of Agreement review	30/11/2017
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Lauri Almond
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved
Version	V5.0

WEISF

Information Sharing Protocol – *DPaRS Programme*

1. Purpose

The Essex Partnership secured £3.3m from the DCLG under the Transformation Challenge Award (TCA) to improve lives for vulnerable adults, children, young people and their families across Essex, delivering fiscal benefits and an increase in public value.

A centre-piece of this programme is the development and use of a new Essex Data Platform to share, match and model pseudonymised data from across partners to improve the support we are able to provide to communities in helping vulnerable people.

The University of Essex has obtained funding from the Higher Education Funding Council of England (HEFCE) under their Catalyst Programme to work with ECC in delivering this project. The University will be bringing to bear their expertise in data science and evaluation to support this project.

We are developing a number of prototypes to test and use the new Essex Data Platform. The first prototype is aimed at improving school readiness in Vange ward in Basildon. By sharing, matching and modelling pseudonymised data, we expect to gain additional insight into the issue of school readiness in Vange that will inform commissioning interventions to support the community in improving outcomes in early years. The insight gained from the Essex Data Platform will be combined with insight from other sources, such as an ethnography project and a community mapping exercise.

2. Information to be shared

The ***pseudonymised*** information to be shared is as follows. Details of each of these variables can be found in the attached file including the unique identifiers to be used for data matching purposes:

1. **Housing and benefits data – Basildon Borough Council**

    - Address
    - Council tax banding
    - % council tax reduction granted/total £ reduction for the year
    - Volume (£) of housing benefits received
    - Housing tenure type
    - Total household arrears

- Social housing flag (yes/no)
- Child benefit flag (yes/no)
- Child tax credits flag (yes/no)
- Family premium (lone parent) (yes/no)
- Claimant incapacity benefit
- Long term family premium
- Claimant employment (gross/net)
- Claimant self-employment (gross/net)
- Weekly earned income disregard
- Weekly amount of childcare disregard

2. Children's social care data – Essex County Council

- Date of birth
- Main address
- Start date known to social care
- End date known to social care

3. School readiness indicators – Essex County Council

- Main address
- School district
- Name
- Gender
- Date of birth
- Ethnicity
- Free school meal (yes/no)
- School name/ID
- Communication and language score
- Physical development score
- Personal, social and emotional development score
- Level of development scores in literacy, mathematics, understanding the world, expressive
- Cumulative school readiness (yes/no) – based on the above score

4. Youth offending service data – Essex County Council

- Address
- Address known to Youth Offending Service (Flag)
- Offence category
- Offence (highest) gravity

5. Drug and alcohol misuse data – Essex County Council

- Address
- In treatment (either: alcohol; opiate; non-opiate; alcohol and non-opiate)
- In treatment within last 12 months

- Successful completion in last 12 months
- Referral source
- Intervention type (pharmacological; psychosocial; recovery support)

6. Police and crime data – Essex Police

- Address
- Offender Address
- Present at household
- Repeat offender
- Anti-Social Behaviour address
- Incident at address flag
- Crime group
- Anti-Social Behaviour Drug related flag
- Anti-Social Behaviour Alcohol related flag
- Anti-Social Behaviour Child present flag
- Anti-Social Behaviour Risk category
- Anti-Social Behaviour Repeat flag
- Domestic Violence Victim address
- Domestic Violence Drug related flag
- Domestic Violence Alcohol related flag
- Domestic Violence Child present flag
- Domestic Violence Risk category
- Domestic Violence Repeat victim flag

3. Legal Basis for Sharing information

It is generally good practice to seek the consent of individuals to share their information. However disclosure may be lawful in certain circumstances without consent, for example the performance of public functions, legal obligations, prevention/detection of crime.

The Data Protection conditions applicable to the processing of this data are:

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions

Anonymised/pseudonymised data only will be shared. No person identifiable data will be used.

If personal data is fully anonymised/pseudonymised it is no longer personal data. In this context anonymised means that it is not possible to identify an individual from the data itself or from that data in combination with other data, taking account of all the means that are reasonably likely to be used to identify them.

ECC will comply with the Health & Social Care Anonymisation Standard and the ICO Anonymisation Code of Practice to ensure that datasets used for this project do not contain personal data.

Fair Processing

Each Partner is responsible for ensuring that Fair processing requirements have been satisfied by being transparent regarding their use of anonymised data for research and service planning in the privacy notices given to individuals at point of contact.

Use of any pseudonymised dataset is for the sole purpose set out above. The Data must not be shared with any other organisation or named individual not explicitly referred to within this protocol.

Publication

Publishing the results of this project and the datasets within the scope of this project and protocol will only take place at the discretion of, and on approval from, ECC and other data owners.

4. Access and individuals' rights

Subject Access is an individual's right to have a copy of information relating to them which is processed by an organisation. As information is being pseudonymised at source, data shared is not subject to section 7 of the Data Protection Act 1998 as it is not defined as personal data.

Essex Partner Agencies' Information Sharing Agreements are made publicly available on the Whole Essex Information Sharing Framework website.

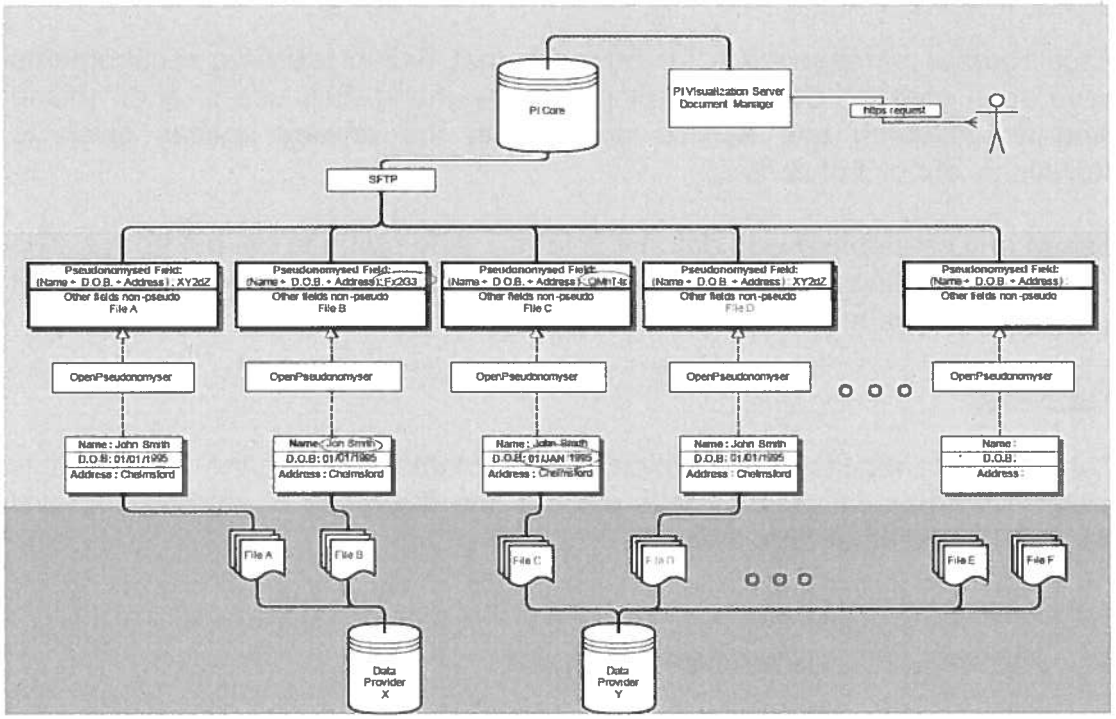
5. Keeping information secure

Pseudonymisation at source is via OpenPseudonymisation provided by University of Nottingham which is compliant with NHS Digital Anonymisation Standard and aligns to the Information Commissioners Office Anonymisation Code of Practice.

Pseudonymised data will be created as a CSV file which can be uploaded by each Partner to an SFTP client hosted by PI.

Once the data matching routine has been completed, results will be hosted by PI and accessed by each Partner via HTTPS.

All data hosted by the supplier is in two UK ISO 27001 certified datacentres and segregated by organisation in a secure database using Nutanix FIPS certified self-encrypted disks. Reference codes and keys will be held by the source organisations and will not be available to the Supplier. Passwords are force changed every 180 days. LDAP and keyclock used for two factor authentication on HTTPS Web Access.



Partners receiving information will:

- Ensure that their employees of 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 up to date policy available to all staff for handling data
- Have a process in place to handle any security incidents including notifying relevant third parties of any incidents

6. Information format and frequency of sharing

The format the information shared is .CSV files via SFTP and HTTPS.

For the purposes of this initial pilot the data collected will be a single instance from each agency.

7. Data Retention

Information will be retained in accordance with each partners' data retention policy and in any event no longer than is necessary.

The data held by the Data Processor, Pi, will be retained until the end of the contractual term of one year, with the provision to extend for a further 3 years, in one year increments and subject to contractual arrangements. At the end of contract, data held by Pi will be securely destroyed in line with contract requirements, and evidenced by log entries provided to ECC by Pi.

8. Responsibility for exchanging these data and ensuring data are accurate

It is incumbent on each Partner to ensure that appropriate data quality assurance checks are made to assure the quality of the data used in this activity. Any Partner who becomes aware of incorrect data must advise all relevant Partners as soon as possible to enable remediation not only at source, but also within the portal.

For the purposes of this Protocol the responsibilities are defined as:

Data Controllers in Common for this Protocol are the Partners listed on the summary page of this document.

"In common" is where data controllers share a pool of personal data, often disclosing data to each other but with each processing the data independently of the other(s). As with 'joint' arrangements, data controllers in common should have written agreements and processes for ensuring that all data controller responsibilities are satisfied. Each needs to exercise due diligence in ensuring that all parties involved are meeting the requirements of law.

Data Processors are PI Limited under contract to Essex County Council.
A data processor can be anyone (other than an employee of the data controller) who processes the data on behalf of the data controller. The Act imposes specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors.

The data controller retains full responsibility for the actions of the data processor – if there is a data protection breach then the data controller remains responsible. The key obligation is that the processing by a data processor must be carried out under a written contract which requires the data processor to act only on instructions from the data controller. In the absence of a written contract a Partner to this protocol will be a data controller in its own right and will need to meet all the requirements of the Data Protection Act 1998.

Partners to this protocol will have the right to independently audit the psuedonymisation activity to assure compliance. This right can be exercised by making a request from one named contact (listed above) to another partner's named contact. The partner receiving the request to audit will make available any of the following:

- An approved Privacy Impact Assessment which details the process by which the partner manages the psuedonymisation of personal data and identifies roles and responsibilities for undertaking the activity
- A procedure document which separately covers the details identified above
- A copy of the pseudonymised dataset which was transferred to the Supplier evidencing that fields containing identifiable data have been processed accordingly.

The right of audit shall not extend to viewing datasets that have not been processed via the psuedonymisation tool.

9. Complaints

Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.

10. Breach of Confidentiality

If the data processor receives any data which has not been fully pseudonymised at source, they must immediately delete the data and inform the provider of the data. Both processor and the provider of the data must work together to identify the cause of the breach using their own internal policies and procedures. Major breaches must be reported to the Information Commissioners Office as soon as is practicably possible.. after consultation with the partners of this protocol.

For any other breaches occurring with the data processed under this protocol, they should be notified to all Partners where their data was involved, and all parties will work together using their own internal policies and procedures to manage the incident, and share any lessons learned with the other Partners.

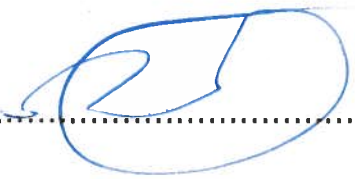
11. Agreement

We undertake to implement and adhere to this protocol.

Signed by:

Position/Job title: EXECUTIVE DIRECTOR PLACE OPERATIONS AND CIO

Print: DAVID WILDE

Signed: 

On behalf of
(Organisation): Essex County Council