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 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		
Supporting Standard Operating Procedure		
Associated contract		
Other associated supporting documentation		

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

INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Safer Communities Research and Evaluation			
Organisation Name	**Head Office Address**	**Telephone**	**Email**	**ICO Registration reference**
Essex Fire and Rescue Service	Kelvedon Park, Rivenhall, Witham, CM8 3HB	01376 576000	foi@essex-fire.gov.uk	Z5349761
University of Essex	Wivenhoe Park, Colchester, CO4 3SQ	0120687 3000	bmorris@essex.ac.uk infoman@essex.ac.uk	Z699129X[1]
Version Control				
Date Agreement comes into force	07/08/2017			
Date of Agreement review	06/08/2018			
Agreement owner (Organisation)	Essex County Fire and Rescue Service			
Agreement drawn up by (Author(s))	Tracy King			
Status of document – DRAFT/FOR APPROVAL/APPROVED	FOR APPROVAL			
Version	V4.0_20170801			

[1] https://ico.org.uk/ESDWebPages/Entry/Z699129X

WEISF

Information Sharing Protocol – Safer Communities Research and Evaluation

1. Purpose

Essex Fire and Rescue Service are committed to being data driven and evidence led. We are keen to evaluate our interventions to understand the effectiveness of them and how we can improve outcomes for the people that we serve and ultimately make Essex a safer place to live and work.

To help us do this at times we will ask partners to assist us with this work. It may be they have access to broader skill set than we do.

The purpose of information sharing under this protocol is to:-

- Facilitate the exchange of sensitive information[2] in the interests of evaluation of our Parish Safety Volunteers initiative. To help us understand what has been achieved, what has been successful and what can we do to improve the Service for our customers to help keep them safer
- Facilitate the exchange of sensitive information in the interest of providing the Service with updated analysis into Accidental Dwelling Fires and Kitchen Fires to assist us with targeting interventions to the right areas of Essex and right people at the right time
- To encourage and develop effective information sharing between different parties and professional groups, based upon trust and understanding.

2. Information to be shared

The information to be shared in relation to the Parish Safety Volunteers Initiative is:

- Location visited to carry out the visit
- Data on when a visit took place by a PSV or a technician by parish, year, month from 2009-2017.
- Time of day visit carried out
- Who carried out the visit i.e. volunteer, technician ect
- Age of people visited
- Sex of people visited
- Health conditions of people visited
- Type of Household
- Who the visit was requested by

2. The information to be shared from the Incident Recording System in relation to the Accidental Fire and Kitchen Fire Analysis is:-

- Incident Number

- Time of call
- Incident Date
- Victims involved
- Persons evacuated
- Alarm system present
- Occupied at time of fire
- Normally occupied
- Cause/motive
- Equipment used
- Main action non FRS
- Main action FRS
- Cause of fire
- Caused by
- Source of ignition
- Household occupancy
- Human factors
- Human factors (Other)
- Suspected under influence
- Fire Classification
- Parish

The original Accidental Fire Report and Kitchen Fire Report will also be supplied.

Mosaic Data Set for Essex 2016

Lower Super Output Boundary File (.shp)

Note that where possible data will cover the years 2009-2017 and will be provided in a Lower Super Output Area level of geography.

3. Legal Basis for sharing information

Sharing this data supports our ability to better understand and address the social determinants of health, risk, behaviour and the mitigating effect of our home safety provision. The primary aim of sharing data in this instance is to better understand the impact of local initiatives that are pioneering new ways of delivering safety information from various organisations, with the ultimate aim of improving safety in the home from fire and crime.

The Data Protection Act 1998

The Data Protection Act 1998 sets out the parameters for sharing information appropriately and safely. Any personal information should be shared on the basis that it is:

- necessary for the purpose for which it is being shared
- shared only with those who have a need for it

- accurate and up to date
- shared securely and in a timely fashion
- not kept for longer than necessary for the original purpose.

In order to comply with the Data Protection Act 1998 (DPA), one requirement is that personal information is shared fairly and lawfully (principle 1). In order to achieve this, organisations must comply with a least one condition from schedule 2 and, where sensitive information is included, at least one condition from schedule 3 of the DPA (Appendix A).

Sharing personal information in accordance with this protocol is lawful under the Data Protection Ac t 1998 schedule 2 condition:

- *The processing is **necessary** –*
  for the exercise of any other functions of a public nature exercised in the public interest.

Sharing personal information in accordance with this protocol is lawful under the Data Protection Act 1998 schedule 3 (d) (if appropriate):

- *The processing –*

  (a) is in the substantial public interest;

Fair Processing

Each partner is responsible for ensuring that Fair Processing requirements have been satisfied by being transparent regarding their use of non-identifiable data for research and service planning in the privacy notices provided to individuals at the point of contact.

Use of the transferred data will be for the purpose set out above, although the parties can review this agreement if a change of need or use is necessary.

Publication

It is understood that outputs of the collaboration will be part of one or more academic publications in the future, and that the University of Essex academics can do so as appropriate subject to:

- Inclusion of any tables/graphs outputs of the data analysis to academic publications will need to adhere to the UK Government Statistical Service guidance for Statistical Disclosure Control[3].

The University of Essex staff will be submitting a copy of the publication to ECFRS for information purposes.

[3] Available from https://gss.civilservice.gov.uk/statistics/methodology-2/statistical-disclosure-control/

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.

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 section 7 of the DPA, unless an exemption applies. It is good practise for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions 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 40 calendar day, time period.

Subject Access requests will be dealt with by each organisation in line with their internal process and procedures. If an organisation receives a Subject Access request relating to the information held by the partner organisation, then the requester will be referred as appropriate to the correct data controller.
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.

FOI and EIR requests will be dealt with by each organisation in line with their internal process and procedures. If an organisation receives a, FOI or EIR request relating to the information held by the partner organisation, then the requester will be referred as appropriate to the correct data controller.

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

5. Keeping information secure

Security for the exchange of information will be achieved through:

- Encryption of all portable devices to industry standard;
- Appropriately marking paper records (for example, "Official-Sensitive");
- Applying other appropriate secure technologies.
- limiting the handover of information to agreed individuals face to face
- assurance from partner organisations about the storage and use of information
- regular meeting regarding the outcome of analysis.

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 personal data
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents

6. Information format, method(s) and frequency of sharing

The format the information shared is likely to be csv or other text based format, Microsoft Office Files (.xls, .xlsx, doc,.docx) and PDFs

The method(s) by which information will be shared will be via email (for non-official, non-sensitive data), secure email (for sensitive data), Encrypted memory stick (following the sector recommendations e.g. AES 256 or greater).or via the Essex County Fire and Rescues secure FTP site.

The frequency with which the information will be shared is One off, with updates to the data as appropriate.

7. Data Retention

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

If information is printed from an electronic system, it will be the partner's responsibility to dispose of the information in a secure manner e.g. cross head shredding or incineration, in line with each Partner's policies.

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

For the purposes of data shared under this protocol, Essex County Fire and Rescue Service are data controllers. Essex University will act as a Data Processor.

Data Controllers are expected to ensure as far as possible that the information they share and receive is accurate; and to differentiate between observations, allegations, facts and opinions.

Data Processors receiving shared information are responsible for applying relevant quality assurance before using the information.

If information is found to be inaccurate, it is the responsibility of Partner discovering the inaccuracy to notify the appropriate data controller. The data controller will ensure that the

source data is corrected and will notify all recipients, who will be responsible for updating the information they hold.

Neither Partner will be liable for any financial or other costs incurred by other parties to this protocol as a result of any information being wrongly disclosed by another party to this protocol or as a result of any negligent act or omission by another party to this protocol.

The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

Everyone sharing data under this agreement is responsible for the quality of the data they are sharing.

Before sharing data, officers will check that the information being shared is accurate and up to date to the best of their knowledge. If sensitive data is being shared which could harm the data subject if it was inaccurate, then particular care must be taken.

If a complaint is received about the accuracy of personal data which affects datasets shared with partners in this agreement, an updated replacement dataset will be communicated to the partners. The partners will replace the out of date data with the revised data.

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

In the event of a breach of confidentiality, staff should contact their organisation's Data Protection Officer/Information Governance team/Legal advisers for advice and guidance. Where a breach is identified as serious, it should be reported to the Information Commissioners Office, as soon as it is practically possible, after informing the partners of this protocol.

All breaches must be recorded and investigated in conjunction with other Partners where relevant, and in accordance with the regulatory requirements.

11. Agreement

We undertake to implement and adhere to this protocol.

Commencement of the 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.

Withdrawal from the Protocol:

Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the other signatories. 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.

Signed by Authorised Person

Print:...Tracy Jane King .....

Signed:.....T King.....

On behalf of (Organisation):...Essex County Fire and Rescue Service.....

Date:...6 September 2017 .....

Signed by Authorised Person

Print:.....Mr Bryn Morris.....

Signed:.....Bry. Morris.....

On behalf of (Organisation):.....Essex University.....

Date:...16.08.17.....

Appendix A: Data Protection Act Conditions for Processing

Sharing non-sensitive[4] personal information in accordance with this protocol is likely to be lawful if at least one of the following circumstances exists (Data Protection Act 1998 **schedule 2 conditions)[5]:**

- *The data subject has given their consent to the processing.*
- *The processing is **necessary** to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*
- *The processing is **necessary** in order to protect the vital interests of the data subject.* In this condition, 'vital interests' refers to matters of life or death.
- *The processing is **necessary** –*
  for the administration of justice;

  for the exercise of any functions conferred by or under any enactment;

  for the exercise of any other functions of a public nature exercised in the public interest.
- *The processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, **except** where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.*

Sharing sensitive[6] personal information in accordance with this protocol is likely to be lawful if at least one of the following circumstances exists in addition to one of the above (Data Protection Act 1998 **schedule 3 conditions**):

- *The data subject has given his **explicit** consent to the processing of the personal data (See Appendix A).*

*The processing is **necessary** –*

[4] For the purposes of this protocol, sensitive personal information is as defined in the Data Protection Act 1998. All other personal information is deemed to be non-sensitive. Information about physical or mental health is classed as sensitive.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

[6] For the purposes of this protocol, sensitive personal information is as defined in the Data Protection Act 1998. All other personal information is deemed to be non-sensitive. Information about physical or mental health is classed as sensitive.

(a) *in order to protect the vital interests of the data subject or another person, in a case where –*
  (i) *consent cannot be given by or on behalf of the data subject, or*
  (ii) *the data controller cannot reasonably be expected to obtain the consent of the data subject, or*

(b) *in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.*

- *The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.*
  The processing –
  (a) *is* ***necessary*** *for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),*
  (b) *is* ***necessary*** *for the purpose of obtaining legal advice, or*
  (c) *is otherwise* ***necessary*** *for the purposes of establishing, exercising or defending legal rights.*

- *The processing is* ***necessary*** *–*
  (a) *for the administration of justice;*
  (b) *for the exercise of any functions conferred by or under any enactment; or the processing is* ***necessary*** *for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by –*
  (a) *a health professional (as defined in section 69 of the Act); or*
  (b) *a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.*

- *The processing –*
  (a) *is of sensitive personal data consisting of information as to racial or ethnic origin;*
  (b) *is* ***necessary*** *for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and*
  (c) *is carried out with appropriate safeguards for the rights and freedoms of data subjects.*

- *The processing –*
  (a) *is in the substantial public interest;*
  (b) *is necessary for the purposes of the prevention or detection of any unlawful act; and*
  (c) *must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.*
- *The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.*

WEISF

Appendix B - Signatories

Organisation Name	ICO	Email
Essex University	Z699129X	bmorris@essex.ac.uk infoman@essex.ac.uk
Essex County Fire and Rescue Service	Z5349761	tracy.king@essex-fire.gov.uk foi@essex-fire.gov.uk