# JOINT INFORMATION SHARING PROTOCOL

## SUMMARY SHEET

| Title of Agreement | Essex Emergency Services Collaboration Data Sharing Protocol |
|---|---|

| Organisation Name | Head Office Address | Phone | Email | Named Data Protection Officer | ICO Notification reference |
|---|---|---|---|---|---|
| PFCCFRA | Kelvedon Park, Rivenhall, Witham, CM8 3HB, Essex | 01376 576000 | Hope.osayande@essex-fire.gov.uk | Hope Osayande | |
| Essex Police | Sandford Rd, Chelmsford CM1 6DN | 101 or 01245 491491 | Adam.Hunt@essex.police.uk | Adam Hunt | |
| Essex Police Fire and Crime Commissioner | Kelvedon Park, Rivenhall, Witham, CM8 3HB, Essex | 01245 291600 | pfcc@essex.police.uk | Suzanne Humphreys | |
| East of England Ambulance Service Trust | East of England Ambulance Service NHS Trust Hammond Road Bedford MK41 0RG | | emma.sears@eastamb.nhs.uk emmasears@nhs.net | Emma Sears | |



PFCC POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX

| Version Control | |
|---|---|
| **Date Agreement comes into force** | May 2020 |
| **Date of Agreement review** | Two years from when signed |
| **Agreement owner (Organisation)** | Essex Police<br>Essex County Fire and Rescue Service<br>East of England Ambulance Service Trust<br>Essex PFCC |
| **Agreement drawn up by (Author(s))** | Mark Johnson (Essex Police), Andy Begent (Essex Police)<br>Hope Osayande and Tracy King (ECFRS)<br>EEAST Emma Sears/Caldecott Guardian |
| **Status of document – DRAFT/FOR APPROVAL/APPROVED** | FOR APPROVAL |
| **Version** | 1.7 |
| **Reason for new version** | Final for Approval – amendments on clarification and process improvements |

# Wider Eastern Information Stakeholder Forum

The Wider Eastern Information Stakeholder Forum (WEISF) is a collaboration of different organisations across Essex that have come together to create a community that supports the development of local information sharing. The WEISF provides a set of good practice principles and template, which are GDPR compliant, to support partners in developing their own Information Sharing Protocols (ISPs), and an online portal to publish ISPs for transparency. An 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 has been developed using the principles of the Wider Eastern Information Stakeholder Forum (WEISF) and applies to all projects within collaboration, covering the Emergency Services of Fire, Police and Ambulance.

This protocol will help identify the issues which need to be considered when deciding whether to share personal data. It should give confidence to share personal data when it is appropriate to do so, but should also give a clearer idea of when it is not acceptable to share data.

Specific benefits to having an ISP include:

- transparency for individuals whose data partners wish to share as protocols are published on the on-line portal;
- 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.

When completed and signed by all partners, published Information Sharing Protocols can be viewed on the WEISF Portal.

| 1. | Purpose | REFERENCES |
|---|---|---|
| The Essex Police Fire and Crime Commissioner, the Chief Constable for Essex Police and the PFCC FRA and the East of England Ambulance Service Trust, are working to improve public safety through more effective co-working, and a more joined-up approach to responding effectively to the most vulnerable groups and individuals. All organisations have a statutory obligation to collaborate under the Policing and Crime Act 2017 to improve Effectiveness, Efficiency, Economy and Public Safety.<br><br>Closer information sharing practice will allow progress towards a whole system approach to public protection, and a whole place approach to commissioning preventative services in response to assessments of threat, risk and harm and vulnerability, and opportunities for enabling business delivery through shared services.<br><br>Whilst Fire and Rescue, Ambulance and Police remain as distinct and separate services, these valuable resources need to work more effectively together and undertake a number of joint initiatives and projects to protect the public and secure best value for money. In order to do this all organisations need to share data and information to undertake these activities, map and realise their benefits and evaluate the success against the criteria laid out in the PFCCs Business Case and meet their statutory duty to collaborate.<br><br>Although the majority of the information sharing will not include personal data e.g. for planning purposes, on occasion some personal data may be shared in the form of risk markers and the relevant home address. | | GDPR<br>Go to article 5 |
| **2.** | **Information to be shared** | |
| • Appropriate sharing of any information when in the public interest, under legal obligation and for vital interest of data subjects, which is necessary and proportionate for the collaborative initiative and in compliance with the law.<br>• Examples of this may include:<br>  ○ Personal Data for the purposes of sharing risk marker information – Unique Property Reference Number (UPRN), names and addresses only.<br>  ○ When we transfer data, we will endeavour to use the UPRN as the unique reference.<br>• The Strategic Outline Case and Business Case templates require specific reference to information sharing, and where this is a requirement of the project, the project managers are required to speak to the appropriate DPO, and detail those discussions and actions arising. | | GDPR<br>Go to articles 6 - 9 |

## 3. Legal Basis

The sharing of personal data will only occur when the following conditions exist:

GDPR
Go to articles 6-14

| Personal Data (identifiable data) | Special Categories of Data (Sensitive identifiable data) |
|---|---|
| General Data Protection Regulation 2016 (GDPR) Article 6: Lawfulness of processing<br><br>https://gdpr-info.eu/art-6-gdpr/ | General Data Protection Regulation 2016 (GDPR) Article 9: Processing of special categories of personal data<br><br>https://gdpr-info.eu/art-9-gdpr/ |
| Vital Interests | Explicit Consent |
| Legal Obligation (Policing and Crime Act 2017) | Vital Interests |
| Public Task | Substantial Public Interest<br>Fire Safety, Crime Prevention, Health, Vulnerability to harm |

## 4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

| For the purposes of this Protocol the responsibilities are defined as follows:<br>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) |
|---|---|---|
| Data Controller for this sharing:<br><br>Each of the parties can act as sole data controller, or one or more may act as joint data controllers, dependant on the requirements of the information sharing required by specific collaborative initiatives.<br>The designated contact points for Individuals are the DPOs:<br><br>PFCCFRA Hope Osayande Hope.osayande@essex-fire.gov.uk<br>Essex Police Adam Hunt Adam.Hunt@essex.police.uk<br>EEAST Emma Sears emma.sears@eastamb.nhs.uk<br>Essex PFCC Suzanne Humphreys pfcc@essex.police.uk | ☒ | PFCCFRA;<br>Essex Police;<br>EEAST;<br>Essex PFCC. |

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 all parties.

## 5. Subject Rights

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.

| **Subject Rights**<br>**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 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. | ☒ |
| 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 | ☒ |

GDPR
Go to articles 12 – 15

GDPR

| | | |
|---|---|---|
| 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. | | Go to article 16 & 22 |
| 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

GDPR articles 30 - 45

The partners agree to put in place appropriate physical, technical and organisational measures to protect any information provided to them under this ISA.

The partners accept the requirement to ensure that any employees are able to access only the shared personal data necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to personal data and Data Protection legislation.

The partners agree to maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.

The partners agree to protect the physical security of the shared information.

The partners agree to protect the electronic security of the shared information.

The partners agree to ensure that all shared information held on portable devices, including laptops, tablets and USB/portable drives, has full disk encryption. This must be to industry standard.

The partners commit to only e-mailing special category personal data and information about individuals' criminal convictions or offences, suspected or otherwise, via secure e-mail.

The partners agree to have contracts and systems in place to ensure that any contractors and subcontractors managing any aspect of information security are fully aware of and abide by this ISA.

| 7. | Format and Frequency | |
|---|---|---|
| The format, means and frequency will be determined by the most appropriate method, depending on the projects, activity (this could include pre-planned operations, safety initiatives) or strategic requirements of Essex Police, East of England Ambulance Service Trust, Essex County Fire and Rescue Service and Essex PFCC | | |
| **8.** | **Data Retention** | |
| Information will be retained in accordance with each partners' published data retention policy available on their websites, and in any event no longer than is necessary. | | GDPR<br>Go to article 5 |
| **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<br>Go to articles 5, 16 - 18 |
| **10.** | **Breach Notification** | |
| • A "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information which we have transmitted or stored or processed.<br>• If the personal data breach occurred in the course of information being shared under this ISA, then the organisation/public body who discovers the breach must **immediately** inform the other partners involved in the sharing of the personal data, particularly the partner who originally shared the information. The email addresses on page 1 should be used to contact the Partners.<br>• The decision to notify the ICO may be made after attempted 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. | | GDPR<br>Go to articles 33, 34, 77 - 84 |

| | |
|---|---|
| • 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.<br><br>• 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.<br><br>• The partners agree to have robust data breach reporting policies in place, and adhere to them, so that all personal data breaches are reported immediately to staff responsible for managing data breaches when such breaches become apparent. Further, partners accept that:<br><br>• Personal data breaches should trigger an exceptional review of this ISA. | |
| **11. Consultation** | |
| • Partners undertake to consult with the originating partner of any shared personal data or other information on the possible harm of disclosure should they receive an FOI, Right of Access, or other application seeking the disclosure of information received by the them from another partner.<br>• Partners undertake to alert one another as per Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing). | GDPR<br>Go to article 19 |
| **12. Complaints / Compliments** | |
| Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol. | GDPR<br>Go to articles 16 – 22 & 77 |

| 13. | 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.

| 14. | Withdrawal from the Protocol | |
|---|---|---|

Any partner may withdraw from this Protocol upon giving written notice to the Essex Emergency Services Strategic Collaboration Governance Board. 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. If withdrawal approved then WEISF administration will be informed.

| 14. | Agreement | |
|---|---|---|

This Protocol must be approved by the responsible person within the organisations (SIRO/Caldecott Guardian/Chief Information Officer).

| | | |
|---|---|---|
| Approver Name (SIRO) | Essex County Fire and Rescue Service SIRO – Tracy King | |
| | Essex Police Deputy Chief Constable – Pippa Mills | |
| | EEAST Medical Director (as Caldecott Guardian) | |
| | PFCC Strategic Head of Policy and Public Engagement – Darren Horsman | |
| Endorsement of support and commitment to this protocol | Roger Hirst,<br>Essex Police Fire and Crime Commissioner and Essex Police Fire and Crime Commissioner Fire and Rescue Authority | |
| | Jo Turton<br>Essex County Fire and Rescue Service CEO / CFO | |
| | Ben-Julian Harrington<br>Essex Chief Constable | |
| | Dorothy Hosein<br>East of England Ambulance Service Trust Chief Executive | |
| Date of Agreement | May 2020 | |