Essex Emergency Services Collaboration Data Protection Impact Assessment (DPIA)

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer
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 Rd Bedford MK41 0RG		emma.sears@eastamb.nhs.uk	Emma Sears

Version Control

Date DPIA comes into force	May 2020
Date of DPIA review	Two years from signing or sooner should there be any significant changes in the processing of personal data
DPIA owner (Organisation)	Essex Police Essex County Fire and Rescue Service East of England Ambulance Service Trust, Essex PFCC
DPIA drawn up by (Author(s))	Mark Johnson (Essex Police), Andy Begent (Essex Police) Hope Osayande (ECFRS) EEAST Emma Sears/Caldecott Guardian
Status of document – DRAFT/FOR APPROVAL/APPROVED	FOR APPROVAL
Version	1.6
Reason for new version	Final for Approval – amendments on clarification and process improvements

1. Introduction

Article 35 of the EU General Data Protection Regulation (2016/679 (GDPR) introduces the concept of a Data Protection Impact Assessment (DPIA). A DPIA (also known as a privacy Impact Assessment) describes the processing of personal data. It also assesses the necessity and proportionality of a processing activity to help manage risks to the rights and freedoms of natural persons resulting from the handling of personal data.

This is a high level DPIA which identifies, at a Programme level, the identification of security risks and how these will be managed.

More specific, project level DPIAs may be created for specific collaborative initiatives, to support this.

2. DPIA Checklist

Does this initiative/processing involve the collection of new information about individuals? **Yes**
Is this information considered personal under GDPR and Data Privacy Legislation? **Yes**
Will the initiative mandate or compel individuals to provide personal information? **No**
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? **Yes**
Will the information collected be stored in or accessed from a geographical location outside of the EEA? **No**
Will personal information be used for a purpose it is not currently used or, or in a way it is not currently used? **Yes**
Does the initiative involve using new technology which might be perceived as being privacy intrusive (e.g. biometrics, facial recognition, etc.)? **Yes**
Will the initiative profile the individual in such a way that can result in making decisions or taking actions that can have significant impact on them? **Yes**
Is the information about individuals of a nature that is likely to raise privacy concerns or expectations (e.g. health records, criminal records or other information that they would consider private? **Yes**
Will the initiative require you to contact individuals in way which they may find intrusive? **No**

3. DPIA Background

Essex County Fire and Rescue Service, East of England Ambulance Service Trust and Essex Police 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. Both organisations have a statutory obligation to collaborate under the Policing and Crime Act 2017 to improve Effectiveness, Efficiency, Economy and Public Safety.

Closer collaboration will include, but is not limited to, ensuring 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.

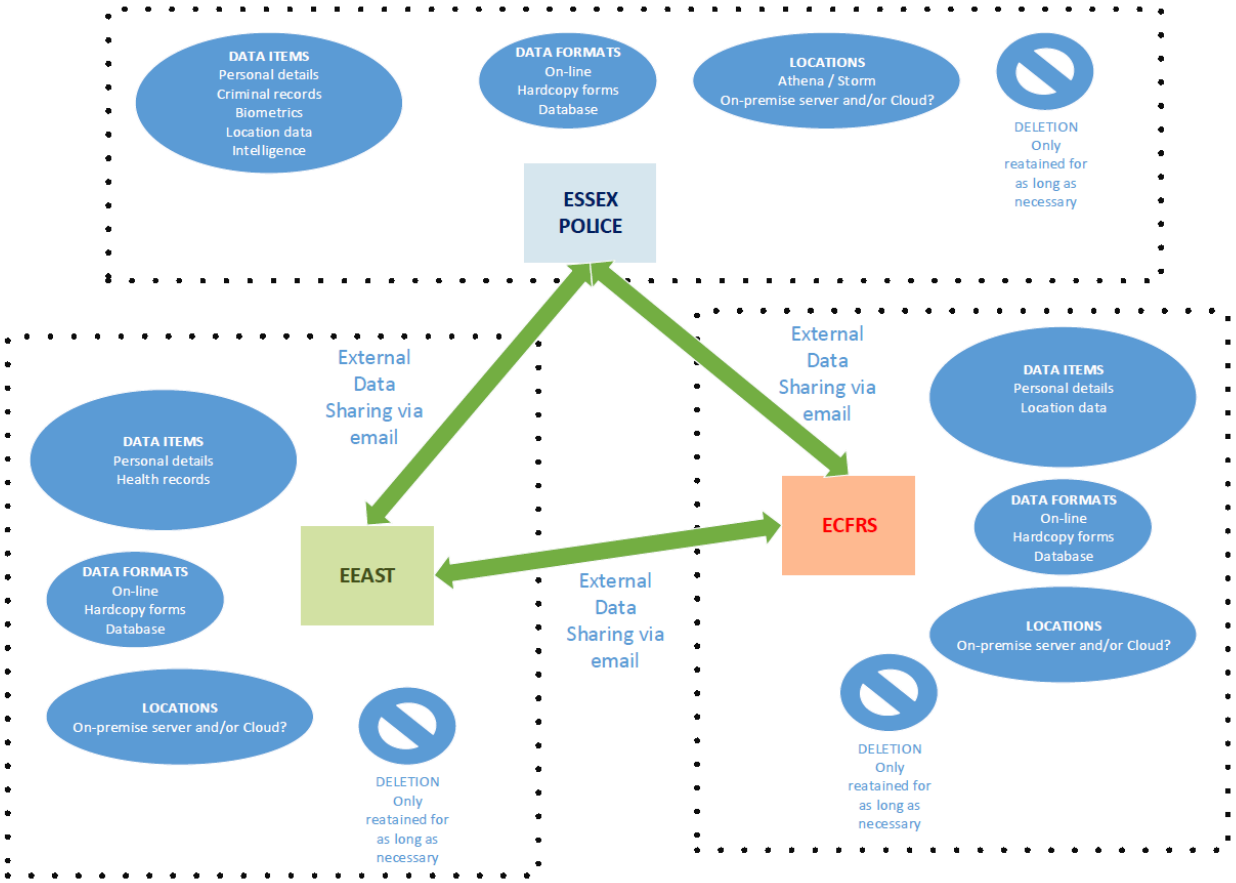
Whilst Fire and Rescue, Ambulance and Police remain as distinct and separate services, these valuable resources need to work more effectively together and undertake a number of joint initiatives and projects to protect the public and secure best value for money. In order to do this all organisations 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.

Although the majority of the information sharing will not include person-identifiable information e.g. for planning purposes, on occasion some person-identifiable information may be shared in the form of risk markers and the relevant home address.

This protocol is need to ensure that all requirements are met under the Data Protection Act 2018.

Data collected may used to ‘signpost’ vulnerable individuals to third party organisations such as social services, housing agencies, LGAs and Active Citizens to help reduce their rick from harm (only in terms of the person-identifiable information shared relating to risk markers).

4. Information Flows



5. Stakeholder Consultation

Please explain how you will go about identifying and addressing privacy risks? Include who the key people or teams that will be consulted internally and externally are as well as how and when the consultation will take place. Consultation is an ongoing process that can be undertaken throughout the DPIA process and afterwards.

- ECFRS Safeguarding Manager and Deputy
- Essex Emergency Services Collaboration Programme Manager
- Essex Emergency Services Collaboration Project Managers
- Essex Police Project Leads
- Essex Police Head of Change Projects and Programmes
- EEAST DPO
- EP DPO
- ECFRS DPO
- EEAST ICT Teams
- EP ICT Teams
- ECFRS ICT Teams
- Essex PFCC DPO

6. Privacy and Related Risks

Use this section as a record of the key privacy risks to individuals and the "Authority".

Privacy Risk	Specific risk to individuals (data subjects)	Compliance Risk	Associated Organisational or corporate risks
Access Control	If inadequate access controls, risk of information being shared inappropriately	Non-compliance with GDPR	Sanctions or fines. Reputational damage to the Service and compensation claims from affected data subjects or individuals
Information retention	If a retention period is not established, information might be used for longer than necessary.	Non-compliance with sector specific legislation and with the storage limitation principle of the GDPR (2016)	Less efficient and streamlined business processes Inability to effectively handle subject access requests….
Information disclosure	Inappropriate disclosure of personal data due to a lack of appropriate controls being in place.	Non-compliance with GDPR	Sanctions or fines. Reputational damage to the Service and compensation claims from affected data subjects or individuals
Sensitive data for vulnerable people	Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.	Non-compliance with GDPR Non-compliance with Safeguarding legislation	Sanctions or fines. Reputational damage to the Service and compensation claims from affected data subjects or individuals
Anonymised data	Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective	Non-compliance with GDPR	Sanctions or fines. Reputational damage to the Service and compensation claims from affected data subjects or individuals
Changes to Project scope	Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project	Non-compliance with GDPR	Sanctions or fines. Reputational damage to the Service and compensation claims from affected data subjects or individuals

LIKELIHOOD OF A DATA BREACH OR INCIDENCE (PROBABILITY)

LEVEL	DESCRIPTOR	CHANCE	DESCRIPTION
1	Very unlikely	0 to 9%	Data breach or incidence may occur only in exceptional circumstances.
2	Unlikely	10 to 29%	Data breach or incidence could occur infrequently.
3	Possible	30 to 69%	Data breach or incidence could occur at some time.
4	Likely	70 to 89%	Data breach or incidence is expected to occur in most circumstances.
5	Certain	90 to 100%	Data breach or incidence will occur in most circumstances.

DATA INCIDENCE OR BREACH SEVERITY (CONSEQUENCE)

LEVEL	DESCRIPTOR	DESCRIPTION
1	Negligible	Mistakes or practices that need to be corrected to entrench an awareness of personal data security. For example, leaving office computers unlocked when away from your desk. Usually results in no data breach.
2	Slight	Incidents involving an individual or a few data subjects that can be easily contacted and resolved.
3	Moderate	A single incident involving about 100 data subjects. No sensitive personal data is compromised. Owners of the personal information will need to be informed. It has the potential to result in a major breach if not mitigated promptly.
4	Major	Data breach involving a substantial amount of personal data. This must be reported to the Information Commissioner's Office (ICO). Owners of the personal information will need to be informed. The Implications can include financial losses/fines to the Service and reputational damage.
5	Catastrophic	Data breach involving personal data that will result in substantial risk to the rights and freedoms of a substantial number of data subjects. Must be reported to the ICO. Owners of the personal information will need to be informed.

RISK ASSESSMENT MATRIX - LEVEL OF RISK

Catastrophic	**5**	**10**	**15**	**20**	**25**
Major	**4**	**8**	**12**	**16**	**20**
Moderate	**3**	**6**	**9**	**12**	**15**
Slight	**2**	**4**	**6**	**8**	**10**
Negligible	**1**	**2**	**3**	**4**	**5**
↑ **Data Breach Severity**	**Very Unlikely**	**Unlikely**	**Possible**	**Likely**	**Certain**
	Data Breach Likelihood →				

Minimal	Tolerable	Moderate	High
If there is an easily applied control measure that is readily available, with negligible resource, implications, it should be applied.	The current system is reasonably satisfactory. Possible minor actions may be required but this nus unlikely.	The present system is unsatisfactory. Further action will be required, prioritised appropriately, thus ensuring that control measures would be implemented. The data processing activity should only take place after the implementation of new controls.	Immediate action must be taken to reduce risk. This would include further data security measures identified and implemented before this activity should take place. The only exception may be where the activity is vital to save human life.

7. Privacy Solutions

RAG status (risk to the rights and freedoms of individuals) – Red = very high, Amber = High, Yellow = Moderate, Green = Low risk.

Risk Description	Rationale and Consequences to / impact on the individual	Existing controls to mitigate Risk HOW	How is the risk to be handled?	Residual Risk (RAG) Status	
				Likelihood	Impact
If inadequate access controls	Risk of information being shared inappropriately	Protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol	Training (new starters and refresher) is part of BAU training in all partners	1	2
If a retention period is not established,	Information might be used for longer than necessary	Retention periods, designed to minimise the length of time that personal data is retained in place	All partners have well embedded and understood protocols	1	3
Inappropriate disclosure of personal data internally within Services due to a lack of appropriate controls being in place.	Risk of information being shared inappropriately	Protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol. Conducting general or project-specific training to ensure that personal data is handled securely	Training (new starters and refresher) is part of BAU training in all partners	1	3
Data anonymisation techniques chosen turn out not to be effective	Information released in anonymised form might lead to disclosure of personal data	Developing an appropriate anonymisation protocol if the use of anonymised data is required.	All partners have well embedded and understood protocols	1	2
Evolution in the nature of the project	Personal data being used in a manner not anticipated by data subjects	Ensuring that individuals are fully informed about how their information will be used if project scope changes	Project doc informs Project Mgrs about the need to refer to DPOs if scope changes	1	3
Vulnerable individuals or individuals sensitive data.	Individuals might be affected to a very high degree by inappropriate disclosure of personal data	Ensuring that individuals are fully informed about how their information will be used Providing a contact point for individuals to raise any concerns they may have with the Services	All partners have well embedded and understood protocols, with information clearly articulated on websites	1	3

8. Signing Off and Recording DPIA Outcomes

Please provide details of who has approved the privacy related risks and describe the solutions identified to address the risks.

Risk	**Approved Solution**	**Approved by** (*Include person's name and position*)
If inadequate access controls	Protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC
If a retention period is not established,	Retention periods, designed to minimise the length of time that personal data is retained in place	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC
Inappropriate disclosure of personal data internally within Services due to a lack of appropriate controls being in place.	Protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol. Conducting general or project-specific training to ensure that personal data is handled securely	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC
Data anonymisation techniques chosen turn out not to be effective	Developing an appropriate anonymisation protocol if the use of anonymised data is required.	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC
Evolution in the nature of the project	Ensuring that individuals are fully informed about how their information will be used if project scope changes	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC
Vulnerable individuals or individuals sensitive data.	Ensuring that individuals are fully informed about how their information will be used Providing a contact point for individuals to raise any concerns they may have with the Services	Tracy King, SIRO, ECFRS DCC Pippa Mills, SIRO Essex Police EEAST Caldicott Guardian. Darren Horsman SIRO Essex PFCC

9. How DPIA outcomes will be integrated into BAU

The DPIA findings and outcomes should be integrated back into the team's day to day way of working. It may be necessary to return to the DPIA at various times. Some departments will benefit from having a more formal review process. The DPIA might generate actions that continue after the DPIA has finished. These should be monitored. Lessons learnt from conducting the DPIA should be recorded for future use.

Please provide who is responsible for integrating the DPIA outcomes back into business as usual and who is responsible for implementing the solutions that have been approved and the contact for any privacy concerns that may arise in future.

Action to be taken	**Date of completion**	**Person responsible**
Implement course of actions identified in the agreement	Defined by each organisation	SIRO