

# WEISF INFORMATION SHARING PROTOCOL

## SUMMARY SHEET



### Title of Agreement: BTUHT A&E Attendance

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
<b>Essex County Council (ECC)</b>	County Hall, Chelmsford, CM1 1QH	08457 430430	<a href="mailto:DPO@essex.gov.uk">DPO@essex.gov.uk</a>	Paul Turner	Z6034810
<b>Mid and South Essex Hospital Group</b>	Basildon &Thurrock University Hospital Nethermayne, Basildon SS16 5NL	01268821957	<a href="mailto:informationgovernance@btuh.nhs.uk">informationgovernance@btuh.nhs.uk</a>	Matt Barker	Z1972899

### Version Control

<b>Date Agreement comes into force</b>	15/08/2021
<b>Date of Agreement review</b>	14/08/2022
<b>Agreement owner (Organisation)</b>	Essex County Council
<b>Agreement drawn up by (Author(s))</b>	ECC Information Governance
<b>Status of document – DRAFT/FOR APPROVAL/APPROVED</b>	APPROVED
<b>Version</b>	1

## Wider Eastern Information Stakeholder Forum

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.

<b>Item</b>	<b>Name/Link /Reference</b>	<b>Responsible Authority</b>
<b>Data Protection Impact Assessment (DPIA)</b>	<b>1126</b>	<b>ECC</b>
<b>Supporting Standard Operating Procedure</b>		
<b>Associated contract</b>		
<b>Associated Policy Documents</b>		
<b>Other associated supporting documentation</b>		

Published Information Sharing Protocols can be viewed on the [WEISF Portal](#).

# 1 – Purpose

ECC Children and Families Commissioning Team are providing Commissioning Support to the Violence and Vulnerability Unit within Essex Police. We have recently commissioned an outside evaluator to provide an evaluation of Basildon and Thurrock University Hospital (BTUH) Youth Workers in Accident & Emergency (A&E) project. This project was created as a US study suggested that intervening with young victims of violence – who are often also perpetrators – in hospitals can both prevent escalation and further violence. Such interventions rely on using a critical point in the young person's life that is both 'teachable' – where the victim's hospitalisation makes them acutely aware of the dangers of their current lifestyle, and therefore more receptive to change – and 'reachable'. Based on the positive outcomes reported for the Redthread programme the Violence and Vulnerability partnership in Essex agreed to allocate Home Office Early Intervention Youth Funding (EIYF) to Essex Youth Service to develop and deliver a 'test and learn' pilot in Basildon and Thurrock University Hospital (BTUH), that would be based on the principles of the Redthread Programme.

The pilot was launched in May 2019 and comprised either 2 ECC youth workers present at Basildon Hospital A&E 3-8pm Mon-Sat to take referrals, or during Covid restrictions to receive referrals from A&E remotely by email from health colleagues. The pilot was initially designed to engage young people who presented as being a victim or perpetrator of violence and to address and disrupt any gang, grooming, child criminal exploitation (CCE) or child sexual exploitation (CSE) activity. The pilot adapted to engage and support young people presenting with wider vulnerabilities.

In 2020 there was an initial evaluation of the project's first year of activity, however this was limited by not being able to match up Basildon Hospital A&E attendance patient level data with Youth Service client level data of Hospital referrals to them and interventions provided by Youth Service to the young person, which would have informed an evaluation of pilot outcomes. The aim of this current evaluation is to test the hypothesis that intervention by Youth Service following young people's A&E attendance can reduce the likelihood of re-attendance. The intention is for the Youth Service to provide BTUHT with the list of patients that A&E have referred to the Youth Service: ID, full name, address with postcode, DOB (or age at referral if DOB not recorded), referral date. BTUHT to match with patient records to extract details of A&E attendances of these young people 1 year before and after referral to Youth Service. BTUHT to provide the independent researcher with this data using only the unique project ID for each patient, and removing other personal information (name, address, and DOB). By this means neither the Youth Service nor the independent researcher will be able to directly link the A&E attendance data with named young people. By using unique project ID but removing personally identifiable data (the young person's full name, date of birth, address, contact details) the independent researcher can receive a pseudo anonymised copy of the Youth Service project spreadsheet to fully analyse, and study the impact of the interventions by the Youth Service on the young people's outcomes, including their A&E attendances.

## 2 – Information to be shared

### From the Youth Service Basildon Hospital Project Spreadsheets for 2019 – 2020 and for 2020 - 2021

Unique Project ID (URN) (ECC to BTUHT)

First Name (ECC to BTUHT)

Last name (ECC to BTUHT)

Date of Birth (ECC to BTUHT)

If DOB not recorded, Age at referral from A&E to Youth Service (ECC to BTUHT)

Date of referral from A&E to Youth Service (ECC to BTUHT)

Full Address (including postcode if provided) (ECC to BTUHT)

### From BTUHT

Unique Project ID (URN) (BTUHT to independent researcher)

Dates of every Basildon Hospital A&E attendance by the young person between 1 May 2018 to present day.

Associated with each A&E attendance date: the reason for A&E attendance, whether arrival by ambulance, whether the A&E attendance leads to hospital admission to a Ward. (BTUHT to independent researcher)

## From the Youth Service to the Independent Researcher

### **2019-2020 spreadsheet**

URN (Youth Service to Independent Researcher)  
Met in A&E? (Youth Service to Independent Researcher)  
Date presented in A&E (Youth Service to Independent Researcher)  
Issue category (Youth Service to Independent Researcher)  
Gender (Youth Service to Independent Researcher)  
Age/DOB (Youth Service to Independent Researcher)  
Work completed by YS (free text field) (Youth Service to Independent Researcher)  
Concerns/Category (Youth Service to Independent Researcher)  
Tier (Youth Service to Independent Researcher)  
Violence, Vulnerable or Other (Youth Service to Independent Researcher)  
Referred to (Youth Service to Independent Researcher)  
Attended with (Youth Service to Independent Researcher)  
Outcomes (Youth Service to Independent Researcher)

### **2020-21, and 2021-22 spreadsheets**

URN (Youth Service to Independent Researcher)  
Met in A&E? (Youth Service to Independent Researcher)  
Date presented in A&E (Youth Service to Independent Researcher)  
Presented with (Youth Service to Independent Researcher)  
Gender (Youth Service to Independent Researcher)  
Age (when referred) (Youth Service to Independent Researcher)  
Activity (free text) (Youth Service to Independent Researcher)  
Concerns/ (Youth Service to Independent Researcher)  
Category (see following 10 categories) (Youth Service to Independent Researcher)  
1 - Health & Well being  
2 - Suicide Risk  
3 - Substance Misuse  
4 - Risk Taking Behaviour

5 - Victims of Violence

6 - Perpetrators of Violence

7 - Grooming

8 - CSE

9 - CCE

10 - NEET/Risk of becoming NEET

Tier (Youth Service to Independent Researcher)

Outcomes (see following list of 10) (Youth Service to Independent Researcher)

1 - (+) engagement with YW

2 - (+) engagement with YP

3 - (+) referral to TYA

4 - (+) referral to YC

5 - (+) referral to NELFT/EWMHS

6 - (+) referral to gangs specific work

7 - (+) referral to other SS in Social care

8 - Improved understanding of risky behaviours

9 - Improved access to education

10 - Reduced attendance @ A&E

Violence, Vulnerable or Other (Youth Service to Independent Researcher)

Referred to (Youth Service to Independent Researcher)

Attended with (Youth Service to Independent Researcher)

Work completed By TYA (Youth Service to Independent Researcher)

### 3. Legal basis

The identified conditions for processing under the Data Protection Act 2018:

Personal Data (identifiable data)	Special Categories of Data (Sensitive identifiable data)
Article 6:	Article 9: (if appropriate):
Public Task	Health & Social Care
Choose an item.	Choose an item.
Choose an item.	Choose an item.
Choose an item.	Choose an item.

Please list below relevant legislation or statute empowering this sharing activity:

### 4. Responsibilities

For the purposes of this Protocol the responsibilities are defined as follows: For help go to <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&amp;from=EN">https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&amp;from=EN</a> Articles 24 – 29 where these roles are explained.	Tick box	Organisation Name(s)
The Sole Data Controller for this sharing is:	<input checked="" type="checkbox"/>	All organisations named above

The Joint Data Controllers for this sharing are:	<input type="checkbox"/>	
In the case of Joint Data Controllers, the designated single contact point for Individuals is:	<input type="checkbox"/>	
Data Processors party to this protocol are (please list):	<input checked="" type="checkbox"/>	Kay Pountney

This Protocol will be reviewed one year after it comes into operation, or sooner should a breach occur or circumstances change, to ensure that it remains fit for purpose. The review will be initiated by the Information Governance Team ECC.

## 5. Data Subject Rights

Partner Agencies' Information Sharing Agreements are made publicly available on the Wider Eastern Information Stakeholder Forum website to enable compliance with article 12 of the GDPR.

It is each Partner's responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. Partners will respond within one month of receipt of a notice to exercise a data subject right. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

<b>Data Subject Rights</b> Select the <b>applicable rights</b> for this sharing according to the legal basis you are relying on	<b>Check box to confirm processes are in place</b>
<b>GDPR Article 13&amp;14 – Right to be Informed</b> – Individuals must be informed about how their data is being used. This sharing must be reflected in your privacy notices to ensure transparency.	<input checked="" type="checkbox"/>
<b>GDPR Article 15 – Right of Access</b> – Individuals have the right to request access to the information about them held by each Partner	<input checked="" type="checkbox"/>
<b>GDPR Article 16 – Right to Rectification</b> – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	<input checked="" type="checkbox"/>
<b>GDPR Article 17 (1)(b)&amp;(e) – Right to be forgotten</b> – 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	<input type="checkbox"/>



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.	
<b>GDPR Article 18 – Right to Restriction</b> – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	<input checked="" type="checkbox"/>
<b>GDPR Article 19 – Notification</b> – Data Controllers must notify the data subjects and other recipients of the personal data under the terms of this protocol of any rectification or restriction, unless it involves disproportionate effort.	<input checked="" type="checkbox"/>
<b>Article 21 – The Right to Object</b> – 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 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.	<input checked="" type="checkbox"/>
<b>Article 22 – Automated Decision-Making including Profiling</b> – the Individual has the right to request that a human being makes a decision rather than a computer, unless it is required by law. The individual also has the right to object to profiling which places legal effects on them.	<input type="checkbox"/>
<b>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.</b> 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.	<input checked="" type="checkbox"/>

## 6. Security of Information

The Partners to this protocol agree that they will apply appropriate technical and organisational security measures which align to the volume and sensitivity of the personal data being processed in accordance with article 32 of the GDPR as applied by the Data Protection Act 2018.

The security of the personal data in transit will be assured by information being sent via secure email and meetings taking place over Teams with only necessary partners being present.

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 3<sup>rd</sup> party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

## 7. Format & Frequency

- The format the information will be shared in is .csv file via SFTP secure transfer.
- The frequency with which the information will be shared is a one off transfer.

## 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. All data beyond its retention will be destroyed securely.

## 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

## 10. Personal Data Breach Notifications

Where a security breach linked to the sharing of data under this protocol is likely to adversely affect an Individual, all involved Partners must be informed within 48 hours of the breach being 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

where notification to the ICO is required it 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 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.

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.

## 11. Complaint Handling

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

## 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](mailto: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 is approved by the responsible person within each organisation (SIRO/Caldicott Guardian/Chief Information Officer).

**Please submit this Protocol to [weisf@essex.gov.uk](mailto:weisf@essex.gov.uk) with a list of approved signatories. The Protocol will then be published on [weisf.essex.gov.uk](https://weisf.essex.gov.uk).**

**Email approvals will only be accepted from an authorised signatory role from each organisation. Please see the list of authorised roles per organisation at <https://WEISF.essex.gov.uk>**