INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Essex Domestic Abuse Partnership's Violence against Women and Girls (VAWG) Evaluation

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Anglia Ruskin University Higher Education Corporation	Bishop Hall Lane, Chelmsford, CM1 1SQ	01245 683696	dpo@anglia.ac.uk	David Humphreys	Z6913835
Essex County Council	County Hall, Chelmsford, CM1 1QH		dpo@essex.gov.uk	Paul Turner	Z6034810

Version Control	
Date Agreement comes into force	11/2/2019
Date of Agreement review	11/2/2020
Agreement owner (Organisation)	Anglia Ruskin University
Agreement drawn up by (Author(s))	David Humphreys
Status of document – DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	1

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 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.

Item	Name/Link /Reference	Responsible Authority
Privacy Impact Assessment (PIA/DPIA)		
Supporting Standard Operating Procedure		
Associated contract	VAWG Data Sharing Agreement	Anglia Ruskin University
Associated Policy Documents		
Other associated supporting documentation		

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

1. Purpose

REFERENCES

The Essex Domestic Abuse Partnership has engaged ARU to evaluate the Violence against Women and Girls (VAWG) programme to inform decision making and planning in relation to future program continuity and improvements. VAWG partners supply personal data for which they are Data Controllers to allow ARU to contact prospective participants to undertake interviews. Analysis of interview responses provides the partners with part of the evaluation of their current services.

GDPR
Go to article 5

2. Information to be shared

GDPR
Go to articles 6 - 9

Agency Name:	**Data field/description**
Applicable to all the Partner Agencies	• Names of beneficiaries
	• Beneficiary contact details (telephone number and/or email address)

3. Legal Basis

GDPR
Go to articles 6-14

General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.

Personal Data (identifiable data)	**Special Categories of Data (Sensitive identifiable data)**	**Criminal offence data**
Article 6:	**Article 9**: (if appropriate):	**DPA Schedule 8** (if appropriate):
Consent	Explicit Consent	Choose an item.
Choose an item.	Choose an item.	Choose an item.
Choose an item.	Choose an item.	Choose an item.

4. Responsibilities

GDPR
Go to articles

For the purposes of this Protocol the responsibilities are defined as follows: 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)	13-14, 24 - 31
The Sole Data Controller for this sharing is:	☐		
The Joint Data Controllers for this sharing are:	☒	The Partners of the Essex Domestic Abuse Partnership	
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Greg Myddleton, Police, Fire & Crime Commissioner for Essex	
Data Processors party to this protocol are (please list):	☒	Anglia Ruskin University	

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 the Essex Domestic Abuse Partnership.

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.

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. 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.

Subject Rights **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
Go to articles 12 – 15

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.	☒	GDPR Go to article 16 & 22
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 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.	☒	
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

Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
Paper information is stored securely	☒	
Paper and electronic information is securely destroyed with destruction log for electronic information	☒	

Laptops and removable media such as memory sticks are secured when not in use	☒
Technical security appropriate to the type of information being processed is applied	☒
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	☒
Disaster recovery arrangements are in place	☒
Encryption of personal data is fully implemented	☒
Data minimisation has been considered	☒
Can pseudonymised or anonymised data be used to meet your processing needs?	☒
There are sufficient access controls for systems/networks in place	☒
Routine and regular penetration tests are carried out	☒
Article 40 Codes of Conduct are adhered to (where applicable)	☐
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	☒
Confirm entry in Records of Processing Activity	☒
Additional measure 1 – please specify here	☐
Additional measure 2 – please specify here	☐

Personal information will be securely shared via*:*

- Secure online survey platform (‘Online Surveys’)
- Password protected email attachments
- Encrypted recording devices
- Secure website upload and download

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

International Transfers (Where applicable)

If any personal data is to be transferred outside of the EEA, please ensure you capture the relevant supporting adequacy decision for such a transfer here (articles 40-43).

Adequacy Decision in place https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en	Date of approval by EU Commission is:	[Provide hyperlink here]
ICO Approved standard contract clauses in place https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf	Date of approval by ICO is:	[Provide hyperlink here]
ICO Approved Binding Corporate Rules in place https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/	Date of approval by ICO is:	[Provide hyperlink here]
The Individuals have given explicit consent to the transfer and understand the risks associated with the transfer	Confirm this consent has been recorded appropriately	√ / ×
The receiving organisation in a 3rd country is bound by an approved Code of Conduct recognised by the EU	Date of approval by ICO is:	[Provide hyperlink here]

ICO guidance on International Transfers can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

7. Format and Frequency

The format the information will be shared in is:

- Existing data:
  - Password protected email file attachments containing:
  - Data regarding delivery and engagement in the intervention (i.e. referrals, engagement, completions, drop-out)
  - Anonymised outcome (i.e. reoffending data and outcome measures/questionnaires) and feedback data from beneficiaries.

The frequency with which the information will be shared is:

There are no plans to repeat this exercise as yet. The project will therefore consist of a single round of transfer of existing data. All other project data will be obtained directly by ARU rather than shared by the Controllers.

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 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 Go to articles 5, 16 - 18

10.	Breach Notification	
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 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. 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		GDPR Go to articles 33, 34, 77 - 84

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.	**Complaints**	
Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.		GDPR Go to articles 16 – 22 & 77
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. 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 must be approved by the responsible person within the organisation (SIRO/Caldicott Guardian/Chief Information Officer).

Approver Name	Paul Bogle
Organisation Name	Anglia Ruskin University Higher Education Corporation
Date of Agreement	5/2/2019

Please submit this Protocol to weisf@essex.gov.uk with list of approved signatories. The Protocol will then be published on 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 on WEISF.essex.gov.uk