INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	3rd Party Access to the Mosaic Social Care System

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall. Chelmsford. CM1 1QH	08457 430430	Informationgovernanceteam@essex.gov.uk	Paul Turner	Z6034810
Action for Children (Multi-Systemic Therapies)	3 The Boulevard Ascot Road Watford WD18 8AG	01923 361 500	stephen.sipple@actionforchildren.org.uk		Z8506252
Anglia Ruskin University (Student Social Workers)	Chelmsford Campus Bishop Hall Lane Chelmsford Essex CM1 1SQ	01245 493131	Jackie.Barlow@anglia.ac.uk		Z6913835
Barnardos (Female Genitalia Mutilation)	Barnardos House Tanners Lane Barkingside Ilford IG6 1QG	01245 299060	Michelle.lee-izu@barnardos.org.uk		Z5951768
Brunel University	Data Protection Officer Brunel University Kingston Lane UXBRIDGE UB8 3PH		data-protection@brunel.ac.uk		Z6640381
Capita Resourcing Limited (HIP & Temp workers)	71 Victoria Street London SW1H 0XA		colin.webster@capita.co.uk		Z9109167
Department for	58 Caswell Close,	07798 635570	lauren.kilbey@dwp.gsi.gov.uk		Z7107614

Works & Pensions (Family Solutions)	Farnborough GU14 8TD				
ECL (Essex Cares Ltd)	Seax House Floor 7 Victoria Road South Chelmsford CM1 1QH	0333 013 9929	Fran.driver@essexcares.org		Z1801658
Essex Partnership University Foundation Trust (EPUT)	Trust Head Office The Lodge Lodge Approach Runwell, Wickford SS11 7XX	01268 555259	Information.governance@eput.nhs.uk		ZA242481
Essex Police	Essex Police Headquarters, PO Box 2, Springfield, Chelmsford, CM2 6DA	01245 491491	Andy.begent@essex.pnn.police.uk		Z4883472
Frontline (Temp Workers)	The DPO The Frontline Organisation 1 Rosebery Avenue London EC1R 4SR	020 3907 7634	dpo@thefrontline.org.uk		ZA133618
London Metropolitan University	Data Protection Officer University Secretary's Office London Metropolitan University 166-220 Holloway Road London N7 8DB		dsar@londonmet.ac.uk		Z636110X
Mid Essex Hospital Service NHS Trust	Broomfield Hospital Court Road Chelmsford Essex CM1 7ET	01268 524900	informationgovernance@btuh.nhs.uk		Z9751505
Middlesex University	Hendon Campus The Burroughs Hendon London NW4 4BT	020 8411 5555	dpaofficer@mdx.ac.uk		Z5439728

National Probation Service	Disclosure team Postal Point 10.38, Floor 10 102 Petty France London SW1H 9AJ United Kingdom		data.access@justice.gov.uk		Z5679958
PA Consulting Services Limited (ASC Digital Program)	10 Bressenden Place London SW1E 5DN		privacy@paconsulting.com		Z6822657
Payerise (Temp Workers)	1st and 2nd Floor 84 Coombe Road New Malden KT3 4QS	0844 371 1977	info@payerise.co.uk		ZA387608
Phoenix Futures (Full Circle)	200 Springfield Road Essex CM2 6LQ	01245 552286	fullcirclechelmsford@hmps.gsi.gov.uk		Z5753869
Pulse (Temp Workers)	Data Protection Officer, ICSG Ltd, 223 Pentonville Road, London N1 9NG	01992 305 720	DPO@pulsejobs.com		ZA240209
Open University	Walton Hall Milton Keynes Bucks, MK7 6AA	01908 653994	data-protection@open.ac.uk		Z5521375
Remedy (HIP)	Connaught House 1st Floor 112-120 High Road Loughton, Essex, IG10 4HJ	020 8502 3933	dataprotection@heritagecare.co.uk		Z4745393
Suffolk University	Waterfront Building Neptune Quay Ipswich IP4 1QJ		dataprotection@uos.ac.uk		Z9376827
Thurrock Council	PO BOX 1 Civic Offices New Road Grays Thurrock Essex RM17 6SL		information.matters@thurrock.gov.uk		Z8228055

University of East Anglia	Norwich Research Park Norwich NR4 7TJ	01603 592431	dataprotection@uea.ac.uk		Z8964916
University of East London	Docklands Campus 4-6 University Way London E16 2RD		dpo@uel.ac.uk		Z6333498
University of Essex	Wivenhoe Park Colchester CO4 3SQ		dpo@essex.ac.uk		Z699129X
University of Hertfordshire	College Lane Hatfield Hertfordshire AL10 9AB		dataprotection@herts.ac.uk		Z5759523

Version Control	
Date Agreement comes into force	20/08/2018
Date of Agreement review	20/08/2019
Agreement owner (Organisation)	Essex County Council
Agreement drawn up by (Author(s))	Lauri Almond
Status of document – DRAFT/FOR APPROVAL/APPROVED	FOR APPROVAL
Version	V2.0

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)	PIA174	Essex County Council
Supporting Standard Operating Procedure	NA	
Associated contract	NA	
Associated Policy Documents	NA	
Other associated supporting documentation	Mosaic Non-Disclosure Agreement	 C4. Mosaic NDA v4.0.doc

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

1. Purpose

REFERENCES

GDPR
Go to article 5

This Protocol supports 3rd party access to the Essex County Council (ECC) Mosaic Social Care System to facilitate partnership working and delivery of commissioned services to ensure that any access to the system is lawful, necessary, proportionate and appropriate.

Any external agency who require their workers to have access to Mosaic in order to deliver services to citizens will be required to sign up to this protocol, and each individual requiring access will be asked to complete an associated non-disclosure agreement (see appendix A). Essex County Council reserves the right to disconnect any user account where access has been abused or is no longer necessary.

Access to the system will be reviewed at least annually. As a part of this process, agencies will be required to confirm that named users still require access the system in order to deliver services to citizens.
It is each Partners responsibility to ensure that ECC are promptly informed when access is no longer required by their employees.

2. Information to be shared

GDPR
Go to articles 6 - 9

The data likely to be shared, but not limited to, is:

Agency Name	Data field/description
All –access to data restricted to what is necessary for the particular purpose	Demographic data, e.g. Name, Address, Date of Birth, Gender
	Assessment data
	Care pathway data
	Safeguarding data
	Involved professionals
	Relationships, e.g. family, friends, care providers, advocates/representatives

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)

Article 6:	Article 9: (if appropriate):
Legal Obligation	Substantial Public Interest
Under Contract	Health & Social Care
Public Task	Choose an item.

Other legislation or statute as follows

- Children Act 1989
- Health and Social Care Act 2015 (For Health/Social Services).
- Human Rights Act 1998
- Equalities Act 2010
- Crime and Disorder Act 1998
- Criminal Justice Act 2003 (Duty to co-operate)
- Police Act 1996 (Code of Practice on the Management of Police Information)
- Housing Act 1996
- Mental Health Act 2007
- Mental Capacity Act 2005
- Localism Act 2011
- Localism Act 2013
- Sex Offenders Act 1997
- NHS and Community Care Act 1990.

The following codes of practice and guidance may also be relevant:

- Common Law Duty of Confidence (Social Services, medical profession, patient confidentiality, Police, Nurses, Health Visitors and Midwives).
- Professional Codes of Conduct
- Confidentiality – NHS Code of Practice November 2003
- Caldicott and Caldicott2 Principles

4. Responsibilities

GDPR
Go to articles 13-14, 24 - 31

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)
The Sole Data Controller for this sharing is:	☐	
The Joint Data Controllers for this sharing are:	☒	
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☒	Essex County Council
Data Processors party to this protocol are (please list):	☒	Mosaic (Servelec) ECL, Action for Children, ASHA – The Hope Rehab Services, Capita Recruitment, Essex Cares Ltd, Frontline, PA Consulting, Phoenix Futures, Payerise, Pulse, Remedy

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 Essex County Council.

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.

Each Partner must ensure that they provide privacy notices at the point of contact and on an ongoing basis in order to meet the obligation to inform data subjects about the use of their personal data.

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 Go to articles 12 – 15
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 Go to article 16 & 22
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 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.	☒ **Only when relying on Public Task as a legal basis**	
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 - please review to ensure that your organisation can meet these standards. If any Partner cannot meet these standards they must advise the Protocol owner, Essex County Council immediately.	
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	☐

GDPR articles 30 - 45

Personal information will be securely shared via secure Mosaic system

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 within 48 hours;
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing;
- Have an active non-disclosure in place for each employee with access to the system.

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 electronic access to the Mosaic system. The frequency with which the information will be shared is as and when necessary for the purpose.		
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, in accordance with the storage limitation principle.		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 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.		GDPR Go to articles 33, 34, 77 - 84
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	
Organisation Name	
Date of Agreement	

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

Appendix A – Mosaic Access Non-disclosure/Access agreement

Information Security and Confidentiality Agreement

In order to have access to information held and owned by Essex County Council I understand that I must comply with relevant legislation and guidance, including:

- The Data Protection Act 2018
- The Data Protection (Subject Access Modification) (Social Work) Order 2011
- The Computer Misuse Act
- The Freedom of Information Act 2000
- The Caldicott Principles
- The Human Rights Act 1998

I understand that I must treat the information held within Essex County Council's Social Care Case Management systems with the strictest confidence and that I must not use, disclose or publish any information form the system other than any activity which is expressly permitted by Essex CC or which is strictly necessary for my work for Essex CC.

I acknowledge that I must not access any information within Essex County Council's Social Care Case Management systems **unless** it is strictly relevant to my work for Essex County Council.

I understand that any disclosure in breach of this agreement may result in access to the system being withdrawn by Essex County Council. It may also be a criminal offence.

Signature…… Date …….

Name	
Job Title	
Team	
Organisation	

This form must be completed before you are given access to Essex County Councils Social Care Case Management Systems.

Further advice or copies of the legislation and guidance mentioned above can be obtained from Essex County Council Information Governance Team who can be contacted on:

Email: informationgovernanceteam@essex.gov.uk

Tel No: 033301 3982