Information Sharing Protocol / Data Sharing Agreement

SUMMARY SHEET

Title of Agreement: Essex Police Access to Social Care Case Management System

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Duke Street, Chelmsford, CM1 1QH	08457 430430	dpo@essex.gov.uk	Paul Turner	Z6034810
Essex Police	New Street Essex Police HQ Chelmsford Essex CM1 1NF		dpo@essex.police.uk	Michelle Watson	Z4883472

Version Control

Date Protocol comes into force	03 July 2024
Date of next Protocol review	03 July 2025
Protocol Lead Organisation	Essex County Council
Protocol drawn up by (Author(s))	Gemma Gibbs, Senior Information Governance Officer
Status– DRAFT/FOR APPROVAL/APPROVED	APPROVED
Version	1.0

Wider Eastern Information Stakeholders 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. We recommend that these protocols are published alongside your online privacy notices for full transparency.

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:

- 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
Data Protection Impact Assessment (DPIA)	1403	Essex County Council
Supporting Standard Operating Procedure		
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

1 – Purpose

Children and Families is recognised as a service in which partnership working can develop and prosper, with a culture of collaboration, integrity and compassion; promoting development and wellbeing of children, young people and their families; protecting them from neglect and abuse.

The activity involves working together with partners delivering a range of early help, family support and effective social work interventions which build resilience, remove barriers and enable children and young people to look forward to a brighter future.

The activity is focused on and responsible for leading the interface between Children`s Social Care and named third Party agencies, by working collaboratively across the children`s system in Essex, to ensure that family intervention is proportionate to need.

This agreement is between Essex County Council and Essex Police specifically.

The activity will allow Essex Police to have access to Children's Social Care case management system (Mosaic) to undertake the following:

- Autonomously collaborate with Advisors and Social Workers within the Children and Families Hub as well as practitioners within their agencies to ensure effective, timely and appropriate triage on Requests for Support (RFS) from their agencies, to inform the lowest level of safe intervention.

- Accountable for providing support and information to practitioners within their own agencies to build on understanding of threshold in line with the Essex Effective Support document and to assist practitioners within their own agencies to develop a deep and consistent understanding of thresholds at Levels 2-3 and when to implement these.

- Develop audit tools that will enable analysis of RFS for Support or Information within their own agencies, give feedback to practitioners on audited practice, contributes to the targeting of resources and the development of a strategy to improve conversion rates within their agencies.

- Participate in any programme to inform collaborative learning to improve practice across Essex.

The information required as part of the activity can only be obtained by access to Mosaic. In order to carry out the checks a named Essex Police Public Protection Intelligence staff member (Intelligence Support Officer x2 and Intelligence Coordinator x1) will be issued with an ECC laptop, which will provide read only access. They are permitted to use the laptop when they are on ECC premises (C&F Hub) or at Essex Police Headquarters. They are **not permitted to use the laptop when working from home.**

Polit Checks

Paedophile Online Investigation Team (POLIT); A specialist police team that protects and prevents children experiencing online abuse. They investigate predatory paedophiles who use the internet to view and distribute indecent images of children and/or incite any other online sexual activity. ECC is granting named Intelligence Officers (Intelligence Support Officer x2 and Intelligence Coordinator x1) to have **read only access** to the social care case management system (using an ECC issued laptop) to carry out the checks directly

Process: The designated Intelligence staff member would conduct the check(s) using an ECC device with access to the Social Care Case Management system. The Intelligence staff member will have undergone relevant training from the Intelligence Coordinator (supervisor) to understand the justification and necessity for completing the check.
Any staff member or officer working on behalf of the Public Protection Intelligence team for these cases (vetted to the same higher level) without access to the system would email the Intelligence Unit Supervisor or designated Intelligence Support Officer to conduct the check on their behalf and will have to provide the justification for the request and an audit reference prior to the check being carried out. The results will be sent by reply email using the Essex Police account.
The information identified by or shared with the Intelligence Support Officer would be a concise summary and restricted to necessary and proportionate information e.g. John SMITH 01/01/2017 is currently open to social care for concerns around sexualised behaviour – case worker is xxx XXX contact details (93843957).

The Intelligence Team will share the information with the POLIT investigating officers. This process is purely to protect children and ensure the information sharing is efficient and effective. This is only in relation to online child sexual abuse and exploitation cases and is therefore a priority

n.b. Where reference is made to *Any staff member or officer working on behalf of the Public Protection Intelligence team* these are members of the Intelligence Coordinator's team and/or any POLIT support officer, as the POLIT staff sometimes work overtime for the Intelligence Coordinator. They are privy to the information when it comes to them and are vetted to a higher level.

2. Information to be shared

- Name
- Address
- Date of birth
- Contact number
- Details of Request for Support or Information made by agency and outcome
- Case status with Children and Families (open/not open)
- Name and contact details of allocated social worker and manage

3. Legal basis

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

Partner to Protocol	Personal Data (identifiable data)	Special Categories of Data (Sensitive identifiable data – if applicable)	Law Enforcement data (if applicable e.g. community safety)
Organisation Name(s)	**Article 6:**	**Article 9: (if appropriate):**	**DPA Part 3 (if appropriate):**
Essex County Council	**Public Task**	**Health & Social Care**	Choose an item.
Essex County Council	Choose an item.	**Substantial Public Interest**	Choose an item.
Essex Police	**Legal Obligation**	**Substantial Public Interest**	**Substantial Public Interest**

Where the data sharing involves Special Category Personal Data or Law Enforcement Data all Partners to the protocol confirm they have an Appropriate Policy Document in place ☒

Please list below relevant legislation or statute empowering this sharing activity: Legislation guides | Local Government Association

Children Act 1989
Working Together to Safeguard Children
Children Act 2004

4. Responsibilities

For help go to Controllers and processors | ICO

DATA CONTROLLERS - Organisation Name(s)	Data Protection Status	Provide Data	Access Data
Essex County Council	**Controller**	☒	☐
Essex Police	**Controller**	☐	☒

DATA PROCESSORS – Organisation Name(s)	Name(s) of Controller managing the Contract or other agreement	DPIA completed
Not applicable		**Choose an item.**

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 Lead Organisation (see page one).

5. Data Subject Rights

All data controllers are responsible for responding to requests to exercise data subject rights received by their organisation.

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. Each Partner has a legal responsibility to ensure they have appropriate processes in place to support the exercising of these rights by Data Subjects.

It should be noted that where the legal condition for processing under this protocol differs for participating organisations, the applicable rights may also vary. It is for each controller to understand which rights apply in respect of the processing condition they rely on.

Data Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	**Check box to confirm processes are in place**
UK 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. Partners are encouraged to publish their sharing protocols alongside their privac**y** notices to support greater transparency.	☒
UK GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner.	☒
UK GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed**.**	☒
UK 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.	☐
UK GDPR Article 18 – Right to Restriction – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☒
UK 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 restriction, unless it involves disproportionate effort.	☒
UK GDPR 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. Individuals always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☒

UK GDPR 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. The individual also has the right to object to profiling which places legal effects on them.	☐
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 public authority that received the request.	☒

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 UK GDPR as applied by the Data Protection Act 2018.

The security of the personal data in transit will be assured by: Named Essex Police Officers will be issued with Essex County Council laptops for read only access to the social care case management system. The laptops will be vanilla build and asset tag details will be held by the C&F Hub management to monitor for retrieval if an EP Officer moves or leaves the organisation. EP Officers must only use the ECC laptop from the ECC Children & Family Hub or at Essex Police Headquarters. EP Officers must not access the ECC laptop at an unsupervised location such as their home. EP Officers will only use secure internal emails between one department to transfer the relevant information. Non-Disclosure agreements will have to be signed prior to issuing ECC laptops and providing access to the SCCM system. All EP Officers will have completed the mandatory data protection training issued by Essex Police to understand their responsibilities when handling the information accessed. EP Officers will only note information that is relevant to the checks being made and random audit checks will be carried out by the management of the ECC Children & Family Hub. Information must not be stored on any individual who has been checked and then disregarded from the investigation.

Partners receiving information will:

- Complete a Data Protection Impact Assessment (DPIA) where necessary
- 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 data breaches involving personal data, including notifying relevant third parties of any breach
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

7. International Transfers **Not Applicable**

8. Format & Frequency

- The format the information will be shared is via read only access to the Social Care Case Management system. EP Officers will not be using ECC laptops to transfer the information. They will use their EP accounts to securely send the relevant information within their network.
- The frequency with which the information will be shared is as required on a case by case basis.

If a shared system is being used by partners:

- What system is being shared? Mosaic – Social Care Case Management system.
- Who is the owner of the system? Essex County Council.
- A DPIA has been completed and approved for the use of this system YES

9. 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 for the purpose of this protocol. All data beyond its retention will be destroyed securely.

10. 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 ☒

11. Personal Data Breach Notifications

Where a data 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 all other affected Partners 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 Lead Organisation as depicted on page one.

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 Lead Organisation as depicted on page one.

All Partners to this protocol must ensure that robust policy and procedures are in place to manage data breaches, including the need to consult Partners where the breach directly relates to information shared under this protocol.

12. Complaint Handling

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

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 4 weeks written notice to the Protocol Lead Organisation stated on page one, who will inform other partners to the protocol. The leaving 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.

15. Agreement

This Protocol has been approved by the responsible person within each organisation (DPO/SIRO/Caldicott Guardian/Chief Information Officer). Email approval and final versions of the protocol will be retained by the Lead Organisation for the lifetime of the Protocol plus two years.

Emails of approval should be sent to the Lead Organisation at: dpo@essex.gov.uk