**WEISF INFORMATION SHARING PROTOCOL**

# SUMMARY SHEET

**Title of Agreement: Southend Essex and Thurrock Child and Adolescent Mental Health Service (SET) (CAMHS)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organisation Name | Head Office Address | Phone | Email | Named Data Protection Officer | ICO Notification reference |
| Essex County Council | County Hall. Chelmsford. Essex. CM1 1QH | 03457 430430 | dpo@essex.gov.uk  | Paul Turner | Z6034810 |
| North East London Foundation Trust | Goodmayes Hospital. Informatics Dept. Barley Lane. Ilford. IG3 8XJ | 0300 5551201 ext. 64393 | rpaley@nhs.net | Robert Paley | Z9096541 |
| HCRG Care Services Ltd | The Heath Business & Technical ParkHeath RoadRuncornWA7 4QX | 0845 504 0594 | ken.thompson@hcrgcaregroup.com | Ken Thompson | Z2823541 |
| Southend City Council | Civic Centre. Victoria Ave. Southend. SS2 6ER | 01702 215000 | Dataprotection@southend.gov.uk  | Valerie Smith  | Z6929331  |
| Thurrock Council | Civic Offices New Road, Grays, RM17 6SL | 01375 652652 | information.matters@thurrock.gov.uk  | Mojeedat Aderinto | Z8228055 |

**Version Control**

|  |  |
| --- | --- |
| Date Protocol comes into force | 01/04/2023 |
| Date of next Protocol review | 31/03/2029 |
| **Protocol Lead Organisation** | Essex County Council |
| Protocol drawn up by (Author(s)) | Lauri Almond |
| Status– DRAFT/FOR APPROVAL/APPROVED | APPROVED |
| Version  | V2.0 |

**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:

* 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) | PIA 303 | ECC |
| Supporting Standard Operating Procedure | NA |  |
| Associated contract | SET CAMHS | Herts and West Essex ICB |
| Associated Policy Documents | NA |  |
| Other associated supporting documentation | NA |  |

1 – Purpose

|  |
| --- |
| The C&YP SET CAMHS Partnership is delivering the service and the partnership covers Health’s 7 place bases which comprises of MSE ICB, the West Essex element of Herts and West Essex ICB, and the northeast Essex element of Suffolk and NE Essex ICB, Essex County Council (ECC), Southend City Council (SCC), Thurrock Council (TC) and NHS England. The vision of this partnership is to improve the mental health of children and young people, aged 0-18, or 25 with SEN when appropriate. The aim being to improve their educational and social life chances by ensuring easy access and the provision of high-quality services that use evidence-based effective interventions through the procurement of a newly integrated Tier 2 & 3 C&YP CAMH service. ECC/SCC/TC and the CCGs have a joint statutory responsibility for the provision of CAMH Services for children and young people in Essex. The parties have agreed that NELFT /ECC/SCC/TC are Data Controllers in Common and that this is the necessary position in order to be compliant with information governance requirements for the Local Authority. The contract was signed, subject to a side note to say that the issue needed to be resolved, although the contract states that, other than for very limited purposes, NELFT is the only authority which is Data Controller. It was always noted that the parties were not in agreement that this was the true legal position. The statutory definition of Data Controller is ‘a person who (either jointly or in Common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.’The legal position relating to local authorities’ sets out that the Local Authority has the right to determine, the purposes for which and the manner in which personal data are processed. This is because Local Authorities have the right to decide how complaints are handled. This is a non-delegable statutory duty which is inherent in Local Government law. Section 26(1) of the Local Government Act 1974 makes it clear that the Council has to retain full accountability for all services which it is the Council’s function to provide. All services are provided as part of the council’s functions. The Local Government Ombudsman has expressed concerns about Local Authority failures to contract appropriately. Therefore, this protocol is to set out the purposes for which the parties now agree that ECC/SCC/TC are the data controller and the circumstances where ECC/SCC/TC will need access to personal data in order to meet its statutory obligations. |

2 – Information to be shared

The information to be shared is broadly those data items listed below, however the list is not exhaustive as the data required will be determined by the reason for access. The sharing of data will be carefully considered on a case-by-case basis and strictly limited to the minimum required to fulfil the justified purposes of sharing of such data.

* **Name (will be provided if known from ECC/SCC/TC and presented to NELFT otherwise it will be the be the below information only)**
* **Date of Birth**
* **Service Provision Dates**
* **Current care pathway**
* **Complaints information (NELFT will always seek consent where possible before releasing complaints information as part of best practice)**

N.B. Full access to clinical notes, created and managed by NELFT, is not required. Only a certain, limited data is required for specific purposes, to enable ECC/SCC/TC to fulfil their statutory duties. The specific purposes include verification of the identification of an individual, dates of their access to services and their care pathway. The reasons for access are likely to be:

* To respond to Local Government Ombudsman complaints;
* to respond to legal challenges, and;
* any other circumstances when we need to access the data to perform statutory functions.

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 – if applicable) | Law Enforcement data (if applicable e.g. community safety) |
| Article 6:  | Article 9: (if appropriate):  | DPA Part 3 (if appropriate):  |
| Public Task | Substantial Public Interest | Choose an item. |
| Legal Obligation | Health & Social Care | Choose an item. |

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

|  |
| --- |
| Children Act 1975, 2004 |
| Education & Skills Act 2008 |
| The Health & Social Care Act 2012 |
| Children & Families Act 2014 |
| Mental Health Act 2007 |
| Mental Capacity Act 2005 |
| Local Government Act 1974 |

4. Responsibilities

|  |  |  |
| --- | --- | --- |
| For the purposes of this Protocol the responsibilities are defined as follows: For help go to [Controllers and processors | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/) | Tick box | Organisation Name(s) |
| The Sole Data Controller for this sharing is: |[ ]   |
| The Joint Data Controllers for this sharing are: |[x]  All parties to this protocol |
| In the case of Joint Data Controllers, the designated single contact point for Individuals is: |[x]  North East London Foundation Trust |
| Data Processors supporting the processing carried out under this protocol are (please list names): |[ ]   |

This Protocol will be reviewed six years after it comes into operation (in line with the contract), 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

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 this ISP to identify which rights apply, and then each Partner has a legal responsibility to ensure they have the appropriate processes in place.

|  |  |
| --- | --- |
| Data Subject RightsSelect the [applicable rights](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-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. | [x]  |
| UK GDPR Article 15 – Right of Access – Individuals have the right to request access to the information about them held by each Partner | [x]  |
| UK GDPR Article 16 – Right to Rectification – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.  | [x]  |
| 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.  | [x]  |
| 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. | [x]  |
| 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 (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing. | [x]  |
| 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. | [ ] N/A |
| 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. | [ ]  N/A |

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: *The use of secure 0365 or equivalent secure email.*

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 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 in is electronic text
* The frequency with which the information will be shared is as and when needed

# 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 [x]

# 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 approvals are retained by the Lead Organisation for the lifetime of the Protocol plus two years.