INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	Thurrock Community Safety Partnership – Information Sharing Protocol

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Thurrock Council	Civic Offices, 2 New Road, Grays, RM17 6SL	01375 652500	Information.matters@thurrock.gov.uk	Lee Henley	Z8228055
Essex Police	West Local Policing Area, Grays Police Station, Brooke Road, Grays, RM17 5BX	101	Terry.Fisher@essex.pnn.police.uk	Michelle Watson	Z4883472
The Probation Service	Carraway House, Durham Road, Laindon, Essex, SS15 6PH	01268 502760	Martin.Lucas@justice.gov.uk	Martin Lucas	Z5679958
Thurrock Clinical Commissioning Group	Civic Offices,		Stephen.mayo@nhs.net	Stephen Mayo	ZA003561

	2nd Floor, New Road, Grays, RM17 6SL				
Essex County Fire and Rescue Service	Kelvedon Park, Rivenhall, Witham, Essex CM8 3HB		Russ.freeman@essex-fire.gov.uk	Russ Freeman	Z5349761

Version Control	
Date Agreement comes into force	with immediate effect
Date of Agreement review	March 2023
Agreement owner (Organisation)	**Thurrock Community Safety Partnership**
Agreement drawn up by (Author(s))	**Michelle Cunningham**
Status of document – DRAFT/FOR APPROVAL/APPROVED	**Draft Review following withdrawal of Essex CRC and change of name for National Probation Service**
Version	V 2.0 Final approved 20th September 2021

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.

Published Information Sharing Protocols can be viewed on weisf.essex.gov.uk/information-sharing-protocols/

1.	Purpose	REFERENCES
Why is the Sharing necessary: To enable Partners within Thurrock Community Safety Partnership (CSP) to share relevant information in order to deliver the CSP priorities outlined within the annual delivery plan which can be accessed via this link https://www.thurrock.gov.uk/community-safety-partnership/thurrock-community-safety-partnership. The CSP will use this data to undertake strategic, tactical and other analysis. **Aims for Sharing:** • To assist the 'policing purpose' - protecting life and property; preserving order; preventing the commission of offences; or bringing offenders to justice. This also includes protecting vulnerable people, or to achieve other legal obligations or duties placed upon Essex Police or its partners. • To set out the partnership between members of the Thurrock Community Safety Partnership, who are signatories to this agreement, and seeks to formalise how those partners share information in achieving their common aims regarding anti-social behaviour, crime prevention and detection and the maintenance of order. • To support the responsibility placed on all partners by the Crime and Disorder Act 1998 to work in partnership with other agencies and individuals to reduce crime and disorder and the Police and Crime Act 2009 placing a duty on Community Safety Partnerships to formulate and implement a strategy to reduce reoffending by adult and young offenders. • Signatory partners also have a legal duty to protect the rights of those individuals who may be affected by information sharing and therefore there is a need for up to date, consistent and valid information sharing protocols. **Benefits of Sharing** This agreement ensures that the sharing of information meets one or more of the Policing purposes. The benefits to the Partnership members are: ○ To prevent incidents of crime, anti-social behaviour, hate/racial incidents and disorder. ○ To identify perpetrators of such incidents. ○ To bring such perpetrators to justice. ○ To protect victims from such perpetrators. ○ To make communities in Thurrock safer		UK-GDPR Go to article 5

2. Information to be shared

(Explain the types of data that you are intending to share. This may need to be quite detailed because in some cases it may be appropriate to share certain details held in a file about someone, but not other special categories of data).

UK-GDPR
Go to articles 6 - 10

Agency Name	Data field/description
1. Essex Police Any police officer serving in the LPA West and Essex Police analysts may share the following types of data where it is lawful and appropriate to do so: Incidents of:	• Anti-social behaviour • Hate crime and incidents • Violence against the person • Domestic abuse • Sexual abuse • Robbery • Relative information in relation to persons linked to gang related violence, drugs and other criminal activity • Drug offences • Public safety and concern • Relative information with regards to concerns with extremism • Burglary and vehicle crime • Theft and handling of stolen goods • Criminal damage • Fraud and forgery
Agency Name	**Data field/description**
2. Thurrock Council Various teams within Thurrock Council may share different types of data in accordance with services they provide. **a. Environment Directorate: community safety and enforcement teams and Public Protection team including trading standards, licensing, and environmental enforcement**	• Intelligence in relation to problem premises linked to gang related violence, drugs, alcohol, CSE, slavery and ASB • Proactive and enforcement activity in relation to individuals and premises

	Incidents in relation to: • Anti-social behaviour • Hate crime and incidents • Environmental crime • Proactive and enforcement activity in relation to individuals and premises		
b. Housing:	• Proactive and enforcement activity in relation to individuals and premises • Information with regards to tenants linked to gang related violence, drugs, alcohol, CSE, slavery and ASB		
c. Adult Social Care:	• Information in relation to those supported by ASC identified as having links to gang related violence, drugs, alcohol, CSE, slavery and ASB		
d. Children's Social Care:	• Information in relation to those supported by CSC identified as having links to gang related violence, drugs, alcohol, CSE, slavery and ASB		
e. PASS Team	• Information in relation to those supported by PASS team identified as having links to gang related violence, drugs, alcohol, CSE, slavery and ASB		
f. Thurrock Youth Offending Service. Information in relation to young offenders including:	• Re-offending rates • Status of offenders i.e. engaging, recalled or in prison • Information in relation to offenders identified as having links to crime, gang related violence, drugs, alcohol, CSE, slavery and ASB		

Agency Name	Data field/description
3. Essex County Fire and Rescue Service **Community Safety & Community Builders teams may share the following types of data:**	• Deliberate primary fires • Deliberate secondary fires • Malicious false alarms to fire service • Information in relation to safeguarding someone from harm
Agency Name	**Data field/description**
4. The Probation Service **Information in relation to high risk offenders** including	• Integrated Offender Management (IOM) • Re-offending rates • Status of offenders i.e. engaging, recalled or in prison • Information in relation to offenders identified as having links to gang related violence, drugs, alcohol, CSE, slavery and ASB
Agency Name	**Data field/description**
	•
Agency Name	**Data field/description**
6. Basildon & Thurrock University Hospital A&E department may share the following types of anonymised data:	• Information on A & E attendances related to assault and violent type injuries by date, time and location if known • Information on A & E attendances related to domestic abuse • Information on A & E attendances related to substance misuse
Agency Name	**Data field/description**
7. Registered Social Landlords Appropriate manager / case worker within each partner who has signed this agreement may share the following types of data:	• Proactive and enforcement activity in relation to individuals and premises • Information with regards to tenants and or premises linked to gang related violence, drugs, alcohol, CSE, slavery and ASB
Agency Name	**Data field/description**

8. Clinical Commissioning Group	• Anonymised information in relation to assaults • Information in relation to mental and behavioural disorders to safeguard from harm • Anonymised Information in relation to substance misuse to safeguard from harm

3. Legal Basis

General Data Protection Regulation 2016 (UK-GDPR) and Data Protection Act 2018

Explain the legal power(s) you have that allow you to share the information

Personal Data	**Special Categories of Data**	**Law Enforcement data (e.g. community safety partnerships)**
Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 6:	Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 9: (if appropriate):	**DPA Part 3** (if appropriate): *[please click and select]*
Legal Obligation	Vital Interests	Substantial Public Interest
Vital Interests	Substantial Public Interest	Administration of Justice
Public Task	Health & Social Care	Vital Interests

Other legislation or statutes that apply are as follows:

- Section 115 Crime and Disorder Act 1998 and Crime and Disorder (prescribed Information) Regulations 2007 s 17, 37, 39(5)
- Section 120 Learning and Skills Act 2000.
- Section 10 & 11 Children Act 2004.
- Section 135, 152 & 153 Housing Act 1996.
- Section 17, 27 &47 Children Act 1989.
- Sex Offenders Act 1997.

• NHS and Community Care Act 1990. • Health and Social Care Act 2001. • Section 110A Social Security Administration Act 1992 • Data Protection Act 2018 • General Data Protection Regulation • Protection from Harassment Act 1997 • Police Reform Act 2002 • Rehabilitation of Offenders Act 1974 • Article 8 Human Rights Act 1998 • Anti-Social Behaviour Act 2003 • Homelessness Act 2002 • Freedom of Information Act 2000 • Criminal Procedures & Investigations Act 1996 • Regulation of Investigatory Powers Act 2000 • Section 20 Immigration & Asylum Act 1999 • Mental Health Act 1983 • Prosecution of Offenders Act 1985 S(6)(1) • Protection of Children Act 1999 • Sexual Offences Act 2003 • Anti-social Behaviour, Crime and Policing Act 2014 **Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.** *To fulfil fair processing requirements under the UK-GDPR, information should be provided to people about how we process their personal data in a concise, transparent, intelligible and easily accessible manner. The information should be written in clear and plain language, particularly if addressed to a child; and will be free of charge* The following privacy information should be provided to data subjects in a notice when we obtain data directly from them: • Identity and contact details of the controller and where applicable the controller's representative and or Data Protection Officer • The purpose of the processing and the legal basis for the processing • The legitimate interests of the controller or third party where applicable • Categories of personal data • Recipient or categories of recipients of the personal data • Details of transfers outside the EEA where applicable and the relevant safeguards • How long the data will be kept for or if this is not set, the criteria used to determine the retention period	UK-GDPR Go to articles 6-14

- The existence of each of the data subject's rights including the right to complain to the ICO and how they may be requested
- Where we rely on consent, information on how consent can be withdrawn at any time
- Where we have not obtained information directly from individuals, the source the personal data originates from and whether it came from publicly accessible sources
- The statutory obligation under which we obtain the personal data and consequences of failing to provide the personal data
- The existence of automated decision making including profiling and information about how decisions are made, the significance and the consequences. [Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a living person, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour , location or movements]

Where the information has not been obtained directly from the data subject the controller shall provide the information above:

- Within a month after obtaining the personal data
- At the point where their personal data is used to communicate with them for the first time
- At the latest when the personal data is first disclosed to another recipient.

Exemptions to Fair Processing

The Fair Processing requirement above will not apply:

- Where the data subject already has the information set out in the list above
- Where the provision of the information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or where it is likely to render impossible or seriously impair the achievement of the objectives of processing under this agreement.
- Where the data controller in this agreement is required by law to obtain or disclose such information and have in place the appropriate measures to protect the data subjects legitimate interests
- Where the personal data must remain confidential in accordance with a statutory obligation or an obligation of professional secrecy regulated by UK law.

Fair processing requirements have been satisfied by:

Thurrock Council – Have an appropriate Privacy Notice https://www.thurrock.gov.uk/privacy on our web page that details what data is collect, when it will be used etc., it also details how a service user can access their data. Our data collection forms also have a small privacy notice on them, linking the service user to the web page if they wish to know more. I feel that we have satisfied the requirement of Article 12.

1. **Essex Police –** The force's privacy notice can be found on the force's website at Privacy notice | Essex Police

All signatories to this agreement are confirming that they have satisfied the requirements of article 12.

4. Responsibilities

UK-GDPR
Go to articles 13-14, 24 - 31

For the purposes of this Protocol the responsibilities are defined as:	√ or ×	Organisation Name(s)
The Sole Controller for this sharing is *A data controller is an organisation that determines the purpose and means of processing the personal data*		
The Joint Controllers for this sharing are: *Where two or more controllers jointly determine the purposes and means of processing, they will be joint controllers. They will in a transparent manner determine their respective responsibilities for compliance with the obligations under the UK-GDPR , in particular with regard to the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by an arrangement between them unless the respective responsibilities of the controllers are determined by* ***Domestic*** *State law to which the controllers are subject. The arrangement may designate a contact point for data subjects*		Thurrock Borough Council Essex Police Clinical Commissioning Group The Probation service Essex Fire & Rescue service
In the case of **Joint Controllers**, the designated contact point for Data Subjects is: *This is to provide a single point of contact for Data Subjects - generally this will be the organisation with ownership of the ISP.*		Michelle Cunningham Thurrock Borough Council
Processors party to this protocol are: *1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*		SERICC Changing pathways Thurrock Lifestyle Solutions BTUH – A & E

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. *3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.* *Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.*		CGL (Wize up) Inclusions EPUT NHS Red Balloon HRA's: Sanctuary Housing Swan Estuary HERA Chelmer HP Peabody Southern Moat Clarion Housing Savilles	

This Protocol will be reviewed biannually to ensure that it remains fit for purpose. The review will be initiated by Michelle Cunningham, Community Safety Partnership Manager, Thurrock Council.

5. Subject Rights

UK-GDPR Article 15 - **Subject Access** - is an individual's right to have a copy of information relating to them which is processed by an organisation and should be referred to the originating organisation where joint data controllers.

Once information is disclosed from one agency to another, the recipient organisation becomes the **Data Controller** for that information. With regards to subject access requests, the **Data Controller** has a statutory duty to comply with article 15 of the UK-GDPR , unless derogation applies. Partners agree not to disclose under subject access personal data derived from another partner without prior warning the originating partner - this would allow, representations to be made to the partner handling the subject access applications should the potential disclosure be harmful and one for which an exemption should be applied preventing disclosure. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory one month (additional 2 months for complex SARs), time period

UK-GDPR
Go to articles 12 – 22

If a party receives a request for information under the **Freedom of Information** (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, 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 under the provisions of the FOI Act or EIR 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.

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 UK-GDPR .

UK-GDPR Article 17 (1)(b)&(e) – **Right to be forgotten** – This right may apply where the sharing is based on consent, 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 to ensure compliance with the UK-GDPR .

UK-GDPR
Go to article 17 & 19

Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	Processes are i place to enact this right - pleas check the box
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.	☒
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 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.	☒		
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

By signing to this agreement organisations agree that the following controls are in place or comment with reasons why not: **Control in place**	√ / ×		UK-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 email networks or using Objective secure where organisations do not have access to secure emails

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
- Have a process in place to handle any data subjects rights request in accordance with the terms of this agreement
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing and on the authorisation and instructions of the data controller

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	Date of approval by EU Commission is:	https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

ICO Approved standard contract clauses in place	Date of approval by ICO is:	https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf
ICO Approved Binding Corporate Rules in place	Date of approval by ICO is:	https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/
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:	UK-GDPR informer.com/UK-GDPR - articles/data-transfers-third-countries

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

7. Format and Frequency

The Frequency of sharing will be determined by individual area and meeting that it is required for and on request.

The format the information will be shared in is as follows

Request and Response – one partner approaches another to request information it believes the other partner holds. This could be via telephone, email, letter or by use of appropriate referral form. The recipient partner would then respond to the requesting partner by the agreed means within 10 working days.

At a Meeting – a formal meeting (with terms of reference, agenda etc.) is held to which partners are invited. The partners attend with their information likely to be of interest to partners. At the start of the meeting a confidentially statement is accepted. During the course of the meeting partners disclose relevant information to one another. Where not relevant to share with all partners this should be disclosed out of the meeting only to those where relevant and proportionate.

Informal Meeting – Direct contact between members of relevant departments i.e. ASB Team, Community Policing team, Licensing officers etc.

Self-Service – Where a Partner is given direct access to Partner(s) IT systems and has the ability to scrutinise information for themselves.

Digital Data Feed – one partner will automatically provide another partner with information digitally via an IT infrastructure, usually on a regular, repeated basis.

ASB case review; information request form – The SPOC for the ASB case review will request all information held by a partner with regards to a review that has been triggered

Central Co-ordinator – The chairs of meetings where personal data is discussed (e.g. Locality Action Group, tasking, gang related violence) will take up the role as central coordinator to whom information is disclosed. The central co-ordinator then uses their judgement to share information to partners where appropriate to do so. The central co-ordinator could also enquire with partners whether they had specific information relevant to a particular issue that they were prepared to share. The CSP manager will act as deputy in the chairs absence.

The frequency with which the information will be shared is ad hoc for personal data in relation to request and response, fortnightly data sharing through locality action groups and Police tasking, quarterly performance data and annually for the purposes of needs assessments and formulation of strategies.

8. Data Retention

Information will be retained in accordance with each partners' published data retention policy and in any event no longer than is necessary.

UK-GDPR
Go to article 5

9. Data Accuracy

Under the UK-GDPR Article 5 personal data shall be accurate and where necessary kept up to date. All partners in this agreement are to take every reasonable step to ensure that inaccurate personal data are erased or rectified without delay.

The data controller has a duty to take every reasonable step to ensure that all recipients of the inaccurate personal data are duly notified.

To fulfil the requirements of Article 5 of the UK-GDPR , all partners and/or agencies in this protocol agree:

- To take every reasonable step to ensure that personal data shared is accurate.
- To take the necessary steps to rectify or erase any inaccurate data without delay
- To take every reasonable step to ensure that all recipients of the inaccurate personal data are duly notified

UK-GDPR
Go to articles 5, 16 - 18

- To ensure that personal data held is kept up to date on a regular basis.

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. Breach Notification

UK-GDPR
Go to articles 33, 34, 77 - 84

Where a security breach linked to the sharing of data under this protocol is likely to adversely affect a data subject, Partners are required to inform all involved Partners within 24 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 rests with the data Controller. Notification to the ICO must be made within 72 hours of the breach being detected.

All involved Partners should consult on the need to inform the Data Subject, 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 ensure that robust policies 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.

A processor is liable for any damage caused by processing, only where it has not complied with obligations of the UK-GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

11. Complaints

UK-GDPR
Go to articles 16 – 22 & 77

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 on the 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

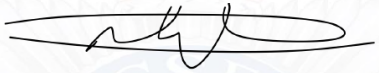
Any partner may withdraw from this Protocol upon giving 4 weeks written notice designated contact point, Michelle Cunningham, who will notify other Partners to the Protocol. The Partner must continue to comply with the terms of this Protocol in respect of any information that the partner has obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate secure manner.

14. Agreement

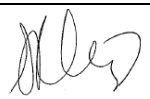
This Protocol must be approved by the responsible person within the organisation (SIRO/Caldicott Guardian/Chief Information Officer).

Approver Name & Signature	Lee Henley 
Organisation Name	Thurrock Council
Date of Agreement	8/10/21

Approver Name & Signature	Julie Rogers 
Organisation Name	Thurrock Council
Date of Agreement	7/10/21

Approver Name & Signature	Mark Barber 
Organisation Name	Essex Police
Date of Agreement	28/9/21

Approver Name & Signature	Ian Adams 
Organisation Name	Essex Fire and Rescue Service
Date of Agreement	11/10/2021

Approver Name & Signature	Stephen Mayo 
Organisation Name	Thurrock Clinical Commissioning Group
Date of Agreement	07/10/2021

Approver Name & Signature	Martin Lucas 
Organisation Name	The Probation Service J12
Date of Agreement	21/09/2021

Please submit this Protocol to weisf@essex.gov.uk with an attached email of approval from the signatory. The Protocol will then be published on weisf.essex.gov.uk.

15 Appendix

This protocol has been signed up to by the responsible person within the following organisations:

Organisation	Name	Signature	ICO Ref
SERICC			
Changing pathways			
Thurrock Lifestyle Solutions			
BTUH – A & E			
CGL Wize up			
Inclusions			
EPUT NHS			
Savilles			
HRA's:			
Sanctuary Housing			
Swan Housing			
Estuary			
HERA			
Chelmer HP			
Peabody			
Southern			
Moat			
Red Balloon			
Clarion Housing			
USP College			

SEC College			