**INFORMATION SHARING PROTOCOL**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Title of Agreement** | | **Essex Health & Justice (No 0133)** | | | | |
| **Organisation Name** | **Head Office Address** | | **Telephone** | **Email** | | **ICO Registration reference** |
| Essex University Partnership NHS Foundation Trust | The Lodge, Lodge Approach, Runwell Wickford Essex SS11 7XX | | 01268 407737 | [Epunft.info.gov@nhs.net](mailto:Epunft.info.gov@nhs.net) | | ZA242481 |
| Castle Rock Group (CRG) | Century House  Suite 5  6th floor  Hardshaw Street  St Helens  Merseyside  Liverpool  LA10 1QU | | 08002118973 | [info@crg.uk.com](mailto:info@crg.uk.com) | | ZA060889+ |
| Phoenix Futures | Phoenix Futures 68 Newington Causeway London SE1 6DF | | 020 7234 9740 | Health.justice.secure@phoenix.cjsm.net | | Z5753869 |
| Essex Police | Essex Police Federation  82 Springfield Road,  Chelmsford  Essex  CM2 6JY | | 01245 491491 | Jo.Collins@essex.police.uk | | Z4678769 |
| CAMHS / NELFT | Ceme Centre Marsh Way Rainham RM13 8EU | | 07967799197 | [tina.russell2@nelft.nhs.uk](mailto:tina.russell2@nelft.nhs.uk) | | Z9096541 |
| Essex County Council  (ASC/AMHPs) | County Hall Chelmsford Essex CM1 1QH | | 07919624565 | [Peter.Devlin@essex.gov.uk](mailto:Peter.Devlin@essex.gov.uk)  DPO@essex.gov.uk 03330139824 | | Z6034810 |
| Southend City Council (ASC/AMHPs) | Data Protection Advisory Service Southend-on-Sea City Council Civic Centre Southend-on-Sea Essex SS2 6ER | |  | [TerryDafter@southend.gov.uk](mailto:TerryDafter@southend.gov.uk) | | Z5950165 |
| Thurrock Council (ASC/AMHPs) | PO BOX 1 CIVIC OFFICES NEW ROAD GRAYS THURROCK ESSEX RM17 6SL | |  | [lbillingham@thurrock.gov.uk](mailto:lbillingham@thurrock.gov.uk) | | Z8228055 |
| East of England Ambulance Service | East of England Ambulance Headquarters Whiting Way Melbourn Cambridgeshire SG8 6EN | | 07740 256071 | Duncan.Moore@eastamb.nhs.uk | | Z955129X |
| Fire and Rescue | Service Headquarters London Road Rivenhall Witham Essex CM8 3HB | | 01245291696 | [suzanne.humphreys@essex.police.uk](mailto:suzanne.humphreys@essex.police.uk) | | Z3451171 |
| British Transport Police | BTPA Ivason House 8a London Bridge Street London SE1 9SG | |  | philippa.smith@btp.pnn.police.uk | | Z1623566 |
| Essex National Probation Service | Head of Public Protection – Probation Service  Millennium House,  Dettingen Way,  Bury St Edmunds,  Suffolk  IP33 3TU | | Ministry of Justice 102 Petty France London SW1H 9AJ dpo@justice.gov.uk | Eoeps.northessex.reception@justice.gov.uk | | Z5679958 |
| Essex HM Courts & Tribunals Services | HM Courts and Tribunals Service, South East Regional Support Unit of 102 Petty France, London SW1H 9AJ | | 07451 081217 | [HMCTSDataIncidents@Justice.gov.uk](mailto:HMCTSDataIncidents@Justice.gov.uk) | | Z5679958 |
| Northampton healthcare NHS Foundation Trust | St Mary Hospital, 77 London Road, Kettering, Northamptonshire, NN15 7PW | | 01536 410141 | mentalhealthinreachteam@nhst.nhs.uk | | Z6769102 |
| **Version Control** | | | | | | |
| **Date Agreement comes into force** | | | | | 1st April 2023 | |
| **Date of Agreement review** | | | | | Annual | |
| **Agreement owner (Organisation)** | | | | | EPUT | |
| **Agreement drawn up by (Author(s))** | | | | | Janet Childs | |
| **Status of document – DRAFT/FOR APPROVAL/APPROVED** | | | | | Approved | |
| **Version** | | | | | 1 | |

**Information Sharing Protocol**

**1. Purpose**

This agreement applies to the organisations listed above operating across the county of Essex and potentially across the borders into other localities where appropriate. The organisations listed above will be referred to within this protocol as ‘partners’. This protocol is for use by professionals, staff or organisations who have agreed and signed it.

The purpose of this information sharing agreement is to enable partners to work together and share information that would otherwise not be freely available, also appropriate sharing of information by partners to effectively prevent harm. Which will allow for enhanced protection of patients, staff and offenders through their interactions with partner organisations.

The Information Sharing Agreement assures the public that the processing of information will be carried out lawfully, fairly and in a transparent manner and in accordance with Data Protection Legislations (the UK General Data Protection Regulation and/or the Data Protection Act 2018).

The purpose of the protocol is to describe what information is required to be shared by partners and to ensure that people who have mental health difficulties, learning difficulties or other vulnerabilities within the criminal justice system are supported through the justice system to ensure the best possible outcome for both the judicial system and for the service user.

Where there is difficulty in managing an individual’s safety, information needs to be shared appropriately and in a timely manner to ensure that the individual’s wellbeing and needs are managed in the least restrictive manner. In certain circumstances, information may include detail to enable partners to undertake their roles effectively and assist in managing challenging behavior.

The information sharing agreement will incorporate the Mental health Street Triage Nurses sharing information to police in circumstances where the police require immediate information on an individual’s risk history and current mental health conditions to determine actions necessary to prioritise the requirement for police attendance based on the potential risk the individual may pose to themselves or others.

This information sharing agreement will also allow agencies to share with each other cohorts of individuals and information regarding identified persons who come into contact with services who are showing indicators of significant risk that suggests they may be at risk of committing a serious violent offence or homicide, which will enable a multi-agency tactical plan to be put in place to mitigate this risk.

Most notably the police will share the following information when there is an indication of serious risk of violence or homicide:

* Police known Domestic Abuse and High Harm individuals, who have a mental health marker. Particularly those individuals where there is increased concern through recency, frequency, and gravity of offending.
* Police known individuals who have come to police attention during dynamic incidents or there are patterns of offending identified and they have been referred into and subject of the SCD review team hot de-brief process.
* Police Force Control Room repeat callers who have been assessed by the FCR Mental Health SPOC and who are showing indicators of increased risk or concern and at risk of serious violence or homicide.
* Police identified suspects who have mental health concerns and come into contact with the Criminal Justice Process, who are showing indicators of increased risk of serious violence or homicide.
* Any highlighted risk police identify as a result that comes into police possession through information or intelligence that suggests as a result of mental health concerns, they might contravene someone else’s right to Article 2 Human rights Act.

The intention of sharing this information is to ascertain whether there is any identified risk held in partner agency data (without contravening patient/personal confidentiality) that would cause Essex Police and partners to consider the impending risk so great that a multi-agency meeting needs to form to mitigate that risk together.

We request from all agencies to share information to enable the police to reduce risk of serious violence and homicide and implement any necessary safeguarding. Specifically, police request that partners share the following data within the scope of this information sharing agreement:

* Any identified risk as a result of mental health in a hospital or community treatment setting, an individual may pose that would mean that another person’s right to Article 2 HRA or personal safety maybe at risk through an offence especially if related to serious violence or homicide whether that person(s) identity is known or not.
* Any discharge of a person from treatment or healthcare setting, whether permanently, temporarily or by day release that poses a risk to themselves or others of committing an offence, especially if related to serious violence or homicide in a community setting. This is to ensure an agreed multi-agency plan is in place to mitigate identified risk factors.
* Any other highlighted risk as a result of mental health that may indicate that someone may be subject to serious violence or a homicide.

Any immediate risk of harm should be raised by the professional through calling 999 and speaking to FCR so the threat can be mitigated at the earliest possible stage.

Any immediate risk of harm that police may identify will result in an urgent call to partner agencies to establish any urgent dynamic information that could assist in mitigating that risk.

In all other matters, and where there is an escalation of risk identified partner information will be shared on a bi-monthly basis.

To govern the process of sharing information between agencies and audit the outputs and outcomes a Mental Health Risk Management Board will be established which is a Multi-Agency Tactical Co-Ordination Group. This will be chaired by the Detective Chief Inspector Operations Centre and held on a bi-monthly basis. A specific Terms of Reference will be formulated to set the direction of the meeting. Any matters that need to be escalated will be referred to the Concordat for review at a Strategic level.

The Information Sharing Agreement is a requirement of the DSPT and meets the best practice guidance of the Information Commissioners Data Sharing Code of Practice. This could consist of data being transferred just once or on an ongoing regular basis, as agreed by the parties involved.

Benefits to the patient will include:

The Health & Justice service workers are based in the Essex police custodies suites and courts throughout Essex. The clinicians from EPUT, CRG and Phoenix Futures identify service users within the criminal justice system and offer a screening/assessment police & courts of any mental, physical health, learning disabilities issues or any other vulnerabilities that are identified, including risk factors in the format of a report. The Street Triage nurses are based in the force control room in police headquarters and attend police related incidences across the county of Essex as well as provide information and advice for police on individuals who are in immediate crisis. The purpose of sharing information is based on current or previous risks of the individual in crisis to ensure that police manage the mental health of the individual in the less restrictive was and look to prevent the detention S136 MHA and attendance to Accident and Emergency (ED) where possible. The benefits of sharing this information is to support the service user and reduce the risk of serious harm to the public by early intervention through multi-agency discussion. Specifically, the benefits are:

* Prevention of serious violence and homicide in the community using sharing information to intervene and prevent by engaging at an earlier stage.
* Prevention and reduction in serious violence against professionals in health settings through consistent partnership engagement.
* Consistent screening and identification of individuals with mental ill health/learning disabilities or other vulnerabilities to ensure they receive appropriate support according to their needs.
* Improved public safety.
* Provision of information to criminal justice agencies to facilitate the earliest possible diversion of offenders with mental disorders from the Criminal Justice system (CJS) and signposting them to local health and social care services as appropriate.
* Better availability of information about a detainee’s previous contact with services.
* Management of information concerning an individual’s mental health needs throughout the criminal justice system (CJS) and back into the community.
* Ensuring continuity in an individual’s mental health care when they are in contact with the CJS.
* Ensure that appropriate information is shared between the agencies that are responsible for caring for an offender with mental health problems/learning disabilities or other vulnerabilities.
* Provide appropriate management and support to individuals with mental ill health/learning disabilities or other vulnerabilities and who are or have been in custody or within the CJS.
* Provide timely and appropriate mental health information in a report format to Essex Police or HM Courts & Tribunals.
* Improved health outcomes for individuals.
* Improved criminal justice outcomes for individuals.
* Improved criminal justice system outcomes.
* Reduction in the number of first-time entrants to the youth justice system.
* Reduce inappropriate use of detention under section 136.

Excelicare is the integrated IT system that is has been put in place for the EPUT nurses that are based within police custodies and courts. CRG & Phoenix Futures staff also use Excelicare; this system has been commissioned by the NHSE commissioners.

All the organisations in the contract use different systems for patient information with EPUT using Paris & Mobius, Phoenix Futures using Theseus system & CRG used only a paper format before Excelicare became live in October 2020. HIE (Health Information Exchange) is a mental health system which holds patient information and is accessible to CRG. HIE is used within the service to share H&J patient information with the rest of EPUT trust staff do not have access to Excelicare.

A number of Police Systems are used in the police to prevent, respond to and investigate incidents and crimes that come to their attention. Primarily, Athena Crime Recording System, ViSOR, and STORM.

To ensure consistency and high standards of governance in place, it is detrimental to the service users for the Health & Justice workers to use the same system and ensure a seamless pathway.

Mental Health Street Triage use systems Mobius and Paris to record their notes and complete a PPU45 screening form to record patient information and daily diary sheets.

The police or courts staff do not have access to Excelicare and any information that the police need regarding a client will be shared with them verbally, written in a report or by making an entry on Athena (police data system) which some of the the nurses have access to.

In all other non-urgent cases the risk of an individual will be raised to the Mental Health Risk Management Board for discussion.

This information Sharing Agreement has been formulated to facilitate the exchange of information between the parties. It must be stressed that all exchange of information must have a legal justification for disclosure and that it is necessary to share the information for one of the purposes outlined above.

**3. Information to be shared with the partners**

3.1

* Name
* Date of birth
* Address
* Social circumstances
* Risk history
* Current risk posed
* Current mental state and mental health/learning disability history
* Family history
* Relationship of mental state to offending
* Treatment options
* Recommendations

*The types of information listed above is not exhaustive and additional information can be shared if certain criteria is met and this will be considered on a case by case basis, as appropriate or need to know.*

**3. Legal Basis for Sharing information**

The purpose of this information sharing agreement is to provide a detailed process for information sharing between the partners.

This information Sharing Agreement is entered into for the purpose of the parties sharing information as required or permitted under the data protection legislation and any other relevant legislation which shall include but not limited to:

* Data Protection Act 2018
* General Data Protection Regulation
* Freedom Of Information Act 2000
* Human Rights Act 1998
* Mental Health Act 1983
* Health and Social Care Act 2012
* Mental capacity Act 2015
* HSCIC Guide to Confidentiality
* Information Governance/Caldicott 2 Review: to share or not to share
* Records Management NHS Code or practice
* NHS England Safe Haven Procedure
* NHS Constitution
* Information Security Management: Code of Practice
* Data Sharing Code of Practice
* Privacy Notices Code of Practice
* Any Other Relevant Legislation, Standards or Guidance

The parties acknowledge and agree that they will share information whenever either or both parties are under a statutory duty to do so. In this case, the party requesting the information shall make clear in its Data Securing Request the legislation underpinning the request for information and the disclosure of information shall comply with the relevant legislation and be made in accordance with the terms of this Information Sharing Agreement, if applicable.

The parties acknowledge and agree that they will not be bound by the terms of this Information Sharing Agreement in the event either or both of them are prohibited to share information by any legislation.

Where it has been identified that the parties are permitted to share information without obtaining consent, this should be justified, if required, under their statutory or legal powers. Data subjects should be made aware of this decision and provided with the details of the data share, unless, by doing this will risk harm to others or hinder any investigation or legal proceeding.

The decision to share information without consent will be fully documented and held within the patients ‘care record’.

It is good practice to seek freely given, specific, informed, and valid consent of individuals to share their information. However, disclosure may be lawful in certain circumstances without consent, for example the performance of public functions, legal obligations, prevention/detection of crime.

*(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the* ***General Data Protection Regulation 2016*** *(GDPR)).*

|  |  |
| --- | --- |
| **Personal Data** | **Special Categories of Data** |
| Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 6(dropdown) | Sharing personal information in accordance with this protocol is lawful under the *General Data Protection Regulation 2016* article 9: (if appropriate): *[please complete]*: |
| *Legal Obligation* | *Article 9(2)(h)* |
| *Legitimate Interests* |  |

**Competent Authorities** (i.e. Essex Police)

Essex Police, and other Competent Authorities, derive their legal basis to disclose, receive and process personal data under this information sharing agreement where the processing meets the definition of law enforcement purposes:

***The prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.***

Where the receiving partner is not a Competent Authority the disclosure must be authorised by law\* (or have the consent of the data subject). Section 115 of the Crime and Disorder Act 1998 provides the lawful power for anyone to disclose information to a Relevant Authority – the police, police authority, local authority, probation committee or health authority, or to any persons acting on their behalf – where this is necessary or expedient for the purposes of a provision of the Act.

Where it is intended to carry out ‘sensitive processing’[[1]](#footnote-1)’ (as detailed in box below), the processing of this sensitive data must be strictly necessary to achieve the specified purpose. Where, strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means. Where the processing does not meet this definition, explicit consent from the data subject must be obtained.

*Sensitive processing:*

*(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;*

*(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;*

*(c) the processing of data concerning health;*

*(d) the processing of data concerning an individual’s sex life or sexual orientation*

**All Other Partners** (including Relevant Authorities)

All Partners, that are not Competent Authorities, are likely to derive their legal basis to disclose, receive and process personal data under this information sharing agreement, from the UK GDPR Article 6(1)(e) *public task.*

Further, Section 115 of the Crime and Disorder Act 1998 provides the lawful power for anyone to disclose information to a relevant authority – the police, police authority, local authority, probation committee or health authority, or to any persons acting on their behalf – where this is necessary or expedient for the purposes of a provision of the Act.

This protocol is recommended to the relevant authorities, as described in the Crime and Disorder Act 1998, as the vehicle to share information to tackle crime and disorder.

Section 115 does not, however, override the need to disclose in a proper manner, considering other statutory and common law constraints on disclosure, including data protection, human rights, and the common law. This Protocol puts in place sound arrangements for information sharing, to be clear about the process involved and the type of information to be shared to ensure compliance with data protection legislation.

Where it is intended to share ‘special category personal data[[2]](#footnote-2)’ (as detailed in box below) and the Partner is relying on a substantial public interest condition[[3]](#footnote-3) or the condition for processing employment, social security and social protection data then an Appropriate Policy Document needs to be in place to cover procedures for ensuring compliance with the law enforcement data protection principles, and policies on the retention and erasure of this data.

Special Category Personal Data:

- personal data revealing racial or ethnic origin;

- personal data revealing political opinions;

- personal data revealing religious or philosophical beliefs;

- personal data revealing trade union membership;

- genetic data;

- biometric data (where used for identification purposes);

- data concerning health;

- data concerning a person’s sex life;

- and data concerning a person’s sexual orientation.

**\*This protocol supports the strategic and statutory responsibilities of all Partner Organisations. Additional specific statutory aspects that apply are:**

* *Section 115 Crime and Disorder Act 1998 and Crime and Disorder (prescribed Information) Regulations 2007 s17, 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*
* *Sections 29 and 3, Data Protection Act 1992*
* *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*
* *Anti-social Behaviour, Crime and Policing Act 2014*
* *Homelessness Act 2002*
* *Criminal Procedures & Investigations Act 1996*
* *Regulation of Investigatory Powers Act 2000*
* *Sec 20 Immigration and Asylum Act 1999*
* *Mental Health Act 1983*
* *Common law duty of confidentiality*
* *Sec 6 (1) Prosecution of Offenders Act 1985*
* *Protection of Children Act 1999*
* *Sexual Offences Act 2003*
* *Housing Act 2004*
* *Public Order Act 1986*
* *Prevention of Abuse and Neglect under the Care Act 2014*
* *Mental Capacity Act 2005*
* The Human Rights Act 1998

Fair Processing in accordance with *General Data Protection Regulation 2016* article 12.

Fair processing requirements have been satisfied by:

Information of both parties’ Fair Processing Notices being either fully available on

their respective publicly available websites or available on request (via electronic or hardcopy):

The information listed above will be available to the data subjects in the following methods:

* EPUT <https://eput.nhs.uk/privacy-policy/>
* CRG <https://crg.uk.com/privacy-policy/>
* Phoenix Futures <https://www.phoenix-futures.org.uk/privacy-cookies-policy/>
* Essex Police <https://www.essex.police.uk/hyg/fpnessex/privacy-notice/>
* HM Courts & Tribunals service <https://www.gov.uk/government/organisations/hm-courts-and-tribunals-service/about/personal-information-charter>
* Northampton Healthcare NHS Foundation Trust - <https://www.northamptongeneral.nhs.uk/InformationAndDataProtection/PrivacyPolicy.aspx>

**4. Access and individuals’ rights**

*(Explain what to do when an organisation receives a DPA or FOI request for access to shared data).*

Subject Access is an individual’s right to have a copy of information relating to them which is processed by an organisation.

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, unless an exemption applies. It is good practise for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual.

If a party receives a request for information under the Freedom of Information (FOI) Act [2000] 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 under the provisions of the FOI Act and to identify any perceived harms. However, the decision to release data under the FOI Act is the responsibility of the agency that received the request.

**5. Keeping information secure**

All information shared between the parties involved in this ISP will be held

in a secure location with limited access and used only for the purposes

listed in this agreement.

* Each party shall ensure that access to information provided by the other

party under this ISP will only be granted to those staff who ‘need to know’ the information.

* The information shared between the parties must not be disclosed to any third party.
* All information held on portable devices must be encrypted to industry standard FIPS 140-2/256-bit asymmetrical encryption
* All data will remain and be stored on servers physically located within the United Kingdom.

Security for the exchange of information will be achieved through a secure - fill in exchange type (e.g secure site, secure nhs.mail to nhs.mail, pnn.police)

Partners receiving information will:

* Ensure their employees can only access the shared information appropriate to their role.
* Ensure that their employees of appropriately trained to understand their responsibilities to maintain confidentiality and privacy.
* Protect the physical security of the shared information.

**6. Information format and frequency of sharing**

The format the information shared is in – tiff, pdf, excel, Microsoft Word.

Shared by Secure email, password protected, nhsmail, pnn.police or verbally.

The frequency with which the information will be shared is an ad-hoc transfer of information

**7. Data Retention**

*(Include detail here how long each organisation will retain the information for).*

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

For the purposes of this agreement, destruction means that data must be irretrievable following destruction or deletion, in accordance with ISO27001 international standard for information security.

The controller will retain information in accordance with the Department of Health’s retention of records schedules.

The processor must not make multiple copies of the data.

The processor shall ensure that the destruction of data will also take place for backup media and provide written confirmation to the controller when destruction has taken place.

**8. Responsibility for exchanging these data and ensuring data are accurate**

Each of the data providers will ensure the accuracy of the data being shared using their own internal quality assurance checks.

For the purposes of this Protocol the responsibilities are defined as:

Caldicott Guardians and Senior Information Risk Owners (SIRO) who have signed the Information Sharing Agreement as having overall responsibility within their own organisation have the duty for ensuring the organisation has the necessary powers to share the information requested. Any information shared must only be used for the purpose as requested.

The parties in discharging their obligations under this information sharing agreement shall comply with the eight data protection principles.

The parties shall ensure that the information shared is relevant and proportionate to the purpose for which it is shared and will comply with the Data Protection Act, information will not be passed to any third party other than allowed by law, retention for the intelligence purposes shall be allowed but only in line with the Data Protection Act.

EPUT have undertaken a privacy impact assessment as under this information sharing agreement information will be shared only where the parties are legally required or permitted to do so.

All parties involved have agreed that the service users (data subjects) need to be informed of the following:

* What information is going to be shared
* In what format is the data going to be exchanged
* Who the information is going to be shared with
* For what purposes it will be used

Unless by doing so would risk harm or self to others or hinder any investigation or legal proceedings.

The Partners agree that the sharing under this ISA will involve processing of personal data which must be carried out in accordance with Data Protection legislation (the General Data Protection Regulation and/or the Data Protection Act 2018).

They agree that some of the personal data may be ‘special category data’ or ‘criminal offence data’ and some of the processing may be ‘sensitive processing’ for which sharing can only occur in narrow circumstances.

The Partners recognise that dependent on their status and the purpose of the processing that some sharing may be processing for law enforcement purposes while some may be for general purposes.

The Partners accept that in terms of Data Protection legislation they are individual controllers in their own right for the personal data held them under this ISA until the point where that information is shared directly with and received by another partner(s) – at that point the recipient partner(s) will assume individual controllership of their copy of the personal data disclosed to them.

The Partners also accept that where information including personal data is ‘pooled’ together from different Partners the pooled information is subject to joint controllership by each partner that has access to that information, as detailed within Article 26 of the UK GDPR.

The Partners accept that they will never use any personal data shared for a purpose that conflicts with or is not compatible with the purpose(s) for which it was shared unless the law allows that to occur.

The Partners agree to only share personal data where it is lawful and fair to do so, subject to exemptions, and where necessary conditions for the processing have been met.

Where Data Processors are a part of this Protocol, the data controller retains full responsibility for the actions of the data processor – if there is a data protection breach then the data controller remains responsible. The key obligation is that the processing by a data processor must be carried out under a written contract which requires the data processor to act only on instructions from the data controller. In the absence of a written contract a Partner to this protocol will be a data controller in its own right and will need to meet all the requirements of the Data Protection Bill and the General Data Protection Regulations 2018.

**9. Complaints**

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

1. **Breach of Confidentiality**

Any reported potential or actual breach of security or inappropriate / unauthorised disclosure of data will be investigated. It is the responsibility of the Data Controller to report the incident following its own internal reporting processes for data breaches.

1. **Agreement**

We undertake to implement and adhere to this protocol.

Signed by Governance Lead

Print: Dr Milind Karale – Caldicott Guardian

Signed:……..………………………………………………………………………….

On behalf of (Organisation): Essex Partnership NHS Foundation Trust

Signed by Governance Lead

Print: Zephan Trent - SIRO

Signed:……..………………………………………………………………………….

On behalf of (Organisation): Essex Partnership NHS Foundation Trust

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:……………………..………………………………………………………….

On behalf of (Organisation): Essex National Probation

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:…………………………………………………………………………………

On behalf of (Organisation): Essex Police

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:…………………………………………………………………………………

On behalf of (Organisation): Castle Rock Group (CRG)

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:…………………………………………………………………………………

On behalf of (Organisation): Phoenix Futures

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:…………………………………………………………………………………

On behalf of (Organisation): Essex HM Courts & Tribunals Services

Signed by Governance Lead

Print:……………………………………………………………………………………

Signed:…………………………………………………………………………………

On behalf of (Organisation): Northampton healthcare NHS Foundation Trust

Definitions

GDPR General Data Protection Regulation

DPA The Data Protection Act

FoIA Freedom of Information Act

Personnal Information “Personal Data” as defined in the above DPB DPA GDPR

Personnel Partner organisations’ employees, officers, elected members, directors, voluntary staff

Consultants and other contractors and their sub-contractors

Sensitive personal data As defined in the above DPB DPA GDPR

Service users Recipients of the partner organisations’ health and care services. Also known as “data subjects” within the meaning of the DPB / DPA1998 / GDPR

ISA’s Information Sharing Agreements

PIA/DPIA Privacy impact assessments

Data Privacy Impact Assessments

SIRO Senior Information Risk Owner

1. S. 35(8) of the DPA 2018 [↑](#footnote-ref-1)
2. UK GDPR Article 9(1) [↑](#footnote-ref-2)
3. Schedule 1 Part 2 of the DPA 2018 [↑](#footnote-ref-3)