|  |  |
| --- | --- |
| Name of Policy | Information Sharing Agreement |
| Version Date | 1st July 2019 |
| Approved by | Nick Roberts, Director of Digital Services, UCLH |
| Date | 1st July 2019 |
| Review Date | October 2019 |
| Target Audience | All data controllers for the Lighthouse including: UCLH, Tavistock and Portman, NSPCC, MOPAC    Partner organisations including Met Police, Solace, Camden Council |
| Authored by | Ikram Musa/Deborah Dillon |
|  |  |

­

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Owner** | **Changes Made** |
| 1.0 | 15/10/18 | Deborah Dillon | Final version developed with partners |
| 1.1 | 19/10/18 | Emma Harewood | Amended LB Camden to Camden Council |
| 1.2 | 01/07/19 | Emma Harewood | Update to info sharing summary to reflect revised method of transfer of evaluation data |

|  |
| --- |
| Lighthouse Policy Statement:  The Lighthouse will provide a coordinated approach to supporting children and young people who have experienced sexual abuse. All medical, advocacy, social care, police, and therapeutic support will be delivered from one place. The aim is that children, young people and their families receive the justice, support and therapy in a timely manner meaning that they can move forward towards recovering from the abuse.  NHS England (London region) in conjunction with MOPAC has commissioned the health and wellbeing services which will be provided by University College London Hospitals (UCLH), The Tavistock and Portman and NSPCC.  Lighthouse procedure and guidance will provide clarity over how staff working within the house will work as part of a multi-agency service, whilst being accountable to their own organisational policies. All Lighthouse policies will be signed off by the Lighthouse Delivery Board which has representation from all agencies. |

This agreement is dated [DATE]

PARTIES

1. **UCLH** incorporated and registered in England and Wales with ICO Registration number: Z8727593 whose registered office is at 250 Euston Road, London, England, NW1 2PG. (Data Discloser)
2. Tavistock and Portman incorporated and registered in England and Wales with ICO Registration number Z1595854 whose registered office is 120 Belsize Ln, London NW3 5BA. (Data Discloser)
3. NSPCC incorporated and registered in England and Wales with ICO Registration number Z6136532 whose registered office is Weston House, 42 Curtain Rd, London EC2A 3NH. (Data Discloser)
4. The Mayor's Office for Policing And Crime (MOPAC) incorporated and registered in England and Wales with ICO Registration number Z2972789 whose registered office is at The Queen's Walk, London SE1 2AA (Data Receiver)

NHS England incorporated and registered in England and Wales with ICO Registration Number Z2950066] whose registered office is at [Quarry House, Quarry Hill, Leeds, LS2 7UE ] (Data Receiver)

1. Solace Women’s Aid incorporated and registered in England and Wales with ICO Registration Number Z1280905 whose registered office is First Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP. (Data Discloser)
2. **Met Police** incorporated and registered in England and Wales with company number [Z4888193 ] whose registered office is at Empress State Building, London, SW6 1TR. (Data Discloser)
3. **London Borough of Camden** incorporated and registered in England and Wales with company number Z5948361 whose registered office is at London Borough of Camden, Town Hall, Judd Street, London, WC1H 9JE (Data Discloser)
4. **Excelicare** incorporated and registered in England and Wales with company number SC179508 whose registered office is at AXSYS HOUSE Marchburn Drive, Glasgow Airport Business Park, Paisley, PA3 2SJ (Data Receiver). A Data Processing Agreement has been published between Excelicare and UCLH.

BACKGROUND

1. The Data Discloser agrees to share the Personal Data with the Data Receiver in the European Economic Area (“EEA”) on terms set out in the Agreement and in the Data Protection Impact Assessment (DPIA).
2. The Data Receiver agrees to use the Personal Data within the EEA on the terms set out in this Agreement.
3. This is a free-standing Agreement that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

AGREED TERMS

1. Interpretation

The following definitions and rules of interpretation apply in this agreement.

* 1. Definitions:

1. Agreed Purpose: has the meaning given to it in clause 4 of this Agreement.
2. Agreement: this Agreement, which is a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.
3. Business Day: Any working day of the week.
4. Commencement **Date**: or “Date” has the meaning given at the beginning of the Agreement.
5. Deletion Procedure: has the meaning given to it in clause 16to this Agreement.
6. Data Sharing Code: The Information Commissioner's Data Sharing Code of Practice of May 2011.
7. **Data Controller** has the meaning in section 1(1) of the Act - “a person who (either alone or 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;”
8. **Data Processor** has the meaning in section 1(1) of the Act – “any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller”;
9. Data Discloser / Data Receiver: for the purposes of this agreement UCLH, Tavistock and Portman, NSPCC, Solace Women’s Aid are the main source of data being disclosed as well as limited case tracking data from Metropolitan Police and social care liaison officers hosted by London Borough of Camden. In reality, data will flow continuously between the parties in order to fulfil the service provided by The Lighthouse. Case management system data is entered into Excelicare and is held on the Excelicare server at RedCentric. Shared drive data is held on a NEL CSU server on the Lighthouse premises and backed up to two NEL CSU off site servers. MOPAC will receive and hold a limited data extract for evaluation purposes. NHS England (London) will receive anonymised service and performance data.
10. Data Protection Legislation: (i) from 25 May 2018 the General Data Protection Regulation as enacted into English law (“GDPR”) as revised and superseded from time to time; (ii) Directive 2002/58/EC as updated by Directive 2009/136/EC; The Data Protection Act 2018 (iii) any other laws and regulations relating to the processing of personal data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant data protection or supervisory authority.
11. **Personal Data Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.
12. Shared Personal Data: the personal data (and special category personal data) to be shared between the parties under clause 8 of this Agreement.
13. Subject Access Request: the exercise by a data subject of his or her rights under Article 15 of the GDPR.
14. **Supervisory Authority**: the relevant supervisory authority in the territories where the parties to this Agreement are established.
15. Term: In line with the Framework Agreement.
    1. **Controller**, **Processor**, **Data Subject** and **Personal Data**, **Special Categories of Personal Data**, **Processing** and "appropriate technical and organisational measures" shall have the meanings given to them in the Caldicott Principles, Data Protection Legislation, DPIA, Data Processing Agreement and EU General Data Protection Regulation principles.
    2. **Data Processing Agreement:** An agreement between The Lighthouse, NEL CSU and Excelicare, identifying the terms of agreement between both parties and ‘appropriate technical and organisational measures’.
    3. **Data Protection Impact Assessment:** Aprivacy-related impact assessment carried out by The Lighthouse whose objective is to identify and analyse how data privacy might be affected by certain actions or activities.
    4. The organisation who have all signed up to The Lighthouse Service may be referred to in this agreement as Partner(s) or Party(ies)
    5. Clause, and paragraph headings shall not affect the interpretation of this Agreement.
    6. Unless the context otherwise, requires, words in the singular shall include the plural and in the plural, shall include the singular.
    7. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.
    8. A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
    9. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.
    10. A reference to **writing** or **written** includes fax and email.
    11. Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.
    12. Children or Young Person (CYP) as referred to in this agreement covers all children and young person/people between the age of 0 – 25.
16. Referenced Documents

The Lighthouse has published the following documents which may be referred to in this agreement.

Data Protection Policy

Data Protection Impact Assessment

Subject Access Request Guideline

Data Processing Agreement

Freedom of Information Guideline

Information Security Policy

Records Management Guideline

Information Handling Procedure

1. Legislations and Principles
   1. Caldicott principles
2. Justify the purpose(s) for using confidential information.
3. Use it only when absolutely necessary.
4. Use the minimum that is required.
5. Access should be on a strict “need to know” basis.
6. Everyone must understand their responsibilities.
7. Understand and comply with the law.
8. The duty to share information can be as important as the duty to protect patient confidentiality.
   1. Data Protection Act 2018 principles
   2. Processing must be lawful, fair and transparent.
   3. Purposes of processing must be specified, explicit and legitimate.
   4. Personal data must be adequate, relevant and not excessive.
   5. Personal data must be accurate and kept up to date.
   6. Personal data must be kept for no longer than is necessary.
   7. Personal data must be processed in a secure manner.
   8. General Data Protection Regulation principles
9. Processed lawfully, fairly and in a transparent manner in relation to individuals.
10. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
11. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
12. Accurate and, where necessary, kept up to date.
13. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
14. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
    1. Lawful Basis for Processing

Yes the processing/sharing personal data for the Lighthouse (Child House) is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

UCLH is an NHS Foundation Trust and lead provider of the Lighthouse Health and Wellbeing services.  The purpose and function of NHS Foundation Trusts is found in National Health Service Act 2006.

1. **National Health Act 2006**

**Chapter 3 Section 25 (i) NHS trusts**

(1)The Secretary of State may by order establish bodies, called National Health Service trusts (“NHS trusts”), to provide goods and services for the purposes of the health service.

<http://www.legislation.gov.uk/ukpga/2006/41/part/2/chapter/3>

**Chapter 5 Section 30 NHS foundation trusts**

1. An NHS foundation trust is a public benefit corporation which is authorised under this Chapter to provide goods and services for the purposes of the health service in England.

<http://www.legislation.gov.uk/ukpga/2006/41/part/2/chapter/5>

 The legal basis for sharing information is found in  **General Data Protection Regulation (GDPR) 2016 and Data Protection Act (DPA) 2018**

**General Data Protection Regulation (GDPR) 2016:**

In order for the sharing/processing of personal data for the **Child House Project** (service for children and young people that experience child sexual abuse) to comply with [GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/) and [DPA Section 86](http://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles/enacted), it must be fair, lawful and transparent, and at least one of the [Article 6](https://gdpr-info.eu/art-6-gdpr/) conditions must be met. [Article 9](https://gdpr-info.eu/art-9-gdpr/) conditions must also be met where special categories of personal data are being shared/processed. Therefore, the following legal bases have been established to unpin to the sharing/processing

GDPR Article 6 Condition:

The processing of personal data in accordance is permitted under the following paragraph:

* [Article 6(1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.](https://gdpr-info.eu/art-6-gdpr/)

GDPR Article 9 Condition

The processing of special categories of personal data is permitted under the following paragraph:

* [Article 9 (2)(h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards](https://gdpr-info.eu/art-9-gdpr/)**.**

Art. 10 GDPR Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

**Data Protection Act (DPA) 2018:**

The lawfulness of processing personal data set out in Article 6(1) (e) of the GDPR (as above) is permitted under [Section 8 (d) of DPA 2018:](http://www.legislation.gov.uk/ukpga/2018/12/section/8/enacted) as NHS Trusts are exercising a function of Department of Health as established under the **National Health Services Act 2006 (see above)**

* Processing is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department.
* The lawfulness of processing special categories of personal data set out in [Article 9 (2) (h)](https://gdpr-info.eu/art-9-gdpr/) of GDPR (as above) is permitted under [DPA Section 10 (health and social care purposes)](http://www.legislation.gov.uk/ukpga/2018/12/section/10/enacted) and, it meets the following conditions set out in [Part 1, Schedule 1 (2)](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted) of DPA:
* [Health or social care purposes](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted) means the purposes of:

1. preventive or occupational medicine;
2. medical diagnosis;
3. the provision of health care or treatment;
4. the provision of social care, or
5. the management of health care systems or services or social care systems or services.

Special categories of personal data: [DPA Section 11(1) supplementary](http://www.legislation.gov.uk/ukpga/2018/12/section/11/enacted)

The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant party’s agencies - which include the police, children’s services authorities, NHS bodies and others must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act also states that they must make arrangements to promote co-operation between relevant party agencies to improve the well-being of children in their area. Well-being is defined by the Act (and was rephrased into ‘outcomes’ in the 2004 Government policy ‘Every Child Matters’) as relating to a child’s:

• physical and mental health and emotional well-being (‘be healthy’);

• protection from harm and neglect (‘stay safe’);

• education, training and recreation (‘enjoy and achieve’);

• the contribution made by them to society (‘make a positive contribution’);

• social and economic well-being (‘achieve economic well-being’).

It will also be necessary to share Personal Identifiable Information with the MOPAC Evidence and Insight team who will evaluate the effectiveness of the Lighthouse through case tracking of health, wellbeing and criminal justice outcomes, to support future funding of the service. Sharing with MOPAC for the evaluation will be explicit consent.

* 1. Information sharing **between NHS bodies and NHS staff** (whether directly employed or not) is also governed by the trust’s Patient and Staff Confidentiality Policy and other advice provided in the information governance portal on Freenet. The trust’s policy on this subject is founded on the Caldicott principles, Data Protection Act 2018 and General Data Protection Regulation. Staff working in the Lighthouse must always abide by the information governance policies, guidance and undertake mandatory IG training of their employing Trust or organisation, as well as the overarching Lighthouse guidance documents and Lighthouse specific IG training.

1. Agreed Purpose
   1. This agreement sets out the framework for the sharing of **Personal Data** between the parties as **Controllers and Processors**. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.
   2. The parties consider this data sharing initiative necessary in order to carry out the services provided by The Lighthouse. This is the purpose of this Agreement.
   3. The parties agree to only process Shared Personal Data, as described in [clause 8] for the following purposes: assessment, case management and tracking (including key dates and milestones in the CJS process), risk management and safeguarding, treatment, therapy and support for children and young people attending the Lighthouse. The parties shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause Agreed Purpose.
   4. The person who will be processing the Information Sharing Agreement and responsible for the Lighthouse Service is the Lighthouse Service Manager.
   5. This agreement will define the structure that will support the exchange of information between the parties.
   6. Each party shall appoint a point of contact(s) (“PoC”) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative.
   7. The points of contact for each of the parties are:

### MOPAC

**Name:** Sara Cain

**Role:** Information Governance Lead

**Telephone Number: 020 7983 6532**

**Email Address: sara.cain@mopac.london.gov.uk**

**Name:** Gareth Linington

**Role:** Programme Manager

**Telephone Number:** 020 7983 4629

**Email Address:** [gareth.linington@mopac.london.gov.uk](mailto:gareth.linington@mopac.london.gov.uk)

### UCLH

**Name:** Emma Harewood

**Role:** Lighthouse Service Manager

**Telephone Number:** 07931249508

**Email Address:** emmaharewood@nhs.net

**Name:** Felicity Hunter

**Role:** Divisional Manager

**Telephone Number:** 02034478873

**Email Address:** felicity.hunter1@nhs.net

**Name:** Deborah Dillon

**Role:** Information Governance Lead

**Telephone Number:** 07971377360

**Email Address:** Deborah.dillon2@nhs.net

### Tavistock and Portman

**Name:** Rob Senior

**Role:** Joint clinical lead for Emotional Health and Wellbeing

**Telephone Number:** 07785521973

**Email Address:** rsenior@tavi-port.nhs.uk

**Name:** S.I Ndumbe

**Role:** Data Security & Protection Manager and DPO

**Telephone Number:** 0208 938 2022

**Email Address:** [Nshu@tavi-port.nhs.uk](mailto:Nshu@tavi-port.nhs.uk)

### NHS England

**Name:** Chloe Collins

**Role:** Senior Commissioning manager

**Telephone Number:**

**Email Address:** chloe.collins6@nhs.net

**Name:** Andrew Bromley

**Role:** Information Governance Role

**Telephone Number:**

**Email Address:** [andrew.bromley2@nhs.net](mailto:andrew.bromley2@nhs.net)

### NSPCC

**Name:** Colin Peak

**Role: Regional head of Service for** London and South East

**Telephone Number:** 02037729862

**Email Address:** [colin.peak@nspcc.org.uk](mailto:colin.peak@nspcc.org.uk)

**Name:** Vacant

**Role:** IG lead

**Telephone Number:**

**Email Address:**

### Solace Women’s Aid

**Name:** Mary Mason

**Role:** Chief Executive Officer

**Telephone Number:**

**Email Address:** m.mason@solacewomensaid.org

### Met Police

**Name:** John Potts

**Role:** T/Head of Information Law and Security

**Telephone Number:** 0207 161 3500

**Email Address:** john.potts@met.pnn.police.uk

**Name:** Richard Smith

**Role:** Head of Profession (Safeguarding)

**Telephone Number:**

**Email Address:** Richard.Smith2@met.police.uk

**Name:** Fiona Martin

**Role:** Temporary Detective Chief Inspector, Child Abuse Investigation Team

**Telephone Number:** 0208 7214226

**Email Address:** [fiona.martin@met.pnn.police.uk](mailto:fiona.martin@met.pnn.police.uk)

### London Borough of Camden

**Name:** Anne Turner

**Role:** Director of Children's Safeguarding and Social Work

**Telephone Number:**

**Email Address: Anne.Turner@camden.gov.uk**

1. Compliance with national data protection laws
   1. Each Party must ensure compliance with applicable national data protection laws at all times during the Term of this agreement.
2. Basis for Sharing
   1. The purpose of this information sharing agreement is to enable the sharing of information for case management, treatment, therapy and support for children and young people attending the Lighthouse, as well as evaluation of the pilot.
   2. The Lighthouse is a programme funded by Home Office, Mayor’s Office for Policing and Crime (MOPAC), NHS England (London region) and Department for Education. The programme aims to radically improve support to children, young people and their non-offending families following incidents of child sexual abuse including exploitation.
3. The aim is to provide a service which is centred around the child. Rather than the child/ young person (CYP) having no choice other than to go to numerous agencies and buildings to access different services The Lighthouse will provide support ‘under one roof’. The environment will be reflective of the circumstances with an emphasis on being safe, secure and focused around the needs of the child/young person.
4. The Lighthouse needs to gather, store and process personal and/or sensitive information about the CYPs or data subjects who access The Lighthouse services. Other parties’ information will also be collected, and they include suppliers, business contacts, employees, key stakeholders (The key ones are University College London Hospital, The Tavistock and Portman NHS Foundation Trust, the NSPCC, Solace Women’s Aid, Metropolitan Police and London Borough of Camden) and other people the organisation has a relationship with or may need to contact. This data will be captured for The Lighthouse to provide a service to the children who been referred to the service. This service can differ on a case-by-case basis but could cover health, justice, support and/or therapy services. This personal data must be processed appropriately whether it is collected on paper, stored in Excelicare case management system, or recorded on other material.
5. In order to provide case management, treatment, therapy, and support and to make the best safeguarding decisions concerning a child or young person and their family, information sharing is an essential part of the Lighthouse service. Information viewed alone or in silos may not give the full picture or identify the true risk.
6. For this reason, Excelicare case management system has been developed as an integrated record with role based system access that allows sharing of:
   1. Registration, referral and appointments details
   2. Initial assessment findings
   3. Risk management and flags
   4. Care plans
   5. Key dates and milestones in the CJS process, including perpetrator status

However, all detailed professional case notes are limited to each profession including:

* 1. Medical and sexual health assessment including full medical history, detailed findings on examination, video recorded genital examinations and sexual health findings
  2. Therapeutic case notes
  3. Advocacy case notes
  4. CJS – Offence details – police only
  5. CJS - PIA and ABE details are limited to police and clinical psychology only

1. Agreement Period
   1. This information sharing agreement will only cover the 2 years ‘pilot’ period. A new agreement will/may be drafted once The Lighthouse program is evaluated and extended. MOPAC will carry out the evaluation and share their findings and evaluation of the program with the partners/parties identified in this agreement.
   2. If the service is recommissioned, then this agreement will need to be reviewed.
2. Shared Personal Data
   1. The following Personal Data may be shared between the parties:
   2. Registration and referral data
      * 1. Name, Address, Gender, Date of birth, Contact Information, ethnicity, GP and school details,
        2. Reason for referral, abuse type, contact details of involved professionals, family background,
   3. Initial assessment including physical health, mental health and advocacy; as well as concluding remarks and key findings,
   4. CJS timeline and outcomes, including dates of ABE, CPS prosecution decision, pre-court preparation, magistrates and crown court trials
   5. Meeting notes and outcomes including strategy meetings, child protection meetings, weekly case review meetings, daily allocation meeting
   6. Risk assessments of each CYP
   7. The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.
   8. This data will only be collected and shared once information sharing has been fully explained to the child/young person and where consent has been provided by the CYP, parent or Guardian where applicable. See section 11: Consent
   9. As all data will be stored on the Excelicare system, the data will be extracted from the system before being shared.
      1. Where applicable, this data may be redacted before being sent out.
   10. The information will only be shared using encrypted emails via NHSmail and GCSX. Where applicable the files may be password protected before being transferred and the password will be sent out separately.
       1. When sending data from an NHS.net account to a non-secure email address the NHS.net [secure] feature must always be used. **Sensitive Personal Information held in paper format must always be stored, transferred and destroyed securely**. Sensitive Personal Information must not be sent using fax unless expressly stated otherwise within this agreement.
   11. All Parties to this Agreement confirm that their security measures on their respective electronic systems that information from Parties may be transferred to are adequate. Information can only be accessed via username and password. Parties confirm that permission to access The Lighthouse information held electronically by Parties will be granted on a strict ‘need-to-know’ basis once it is contained within each Parties electronic systems.
   12. It is not the intention of this Agreement that information will be produced in a hard format. If information is printed off from an electronic system, it will be the Parties’ responsibility to keep the information secure by measures such as storing documents in a locked container when not in use. Access to printed documents must be limited only to those who legitimately ‘need to know’ that information. There should also be a clear desk policy where Parties’ information, and personal information in particular, is only accessed when needed and stored correctly and securely when not in use.
3. Access to Data
   1. Each organisation will have varied roles with regards to data discloser and data receiver. See Appendix A for Lighthouse data sharing summary.
   2. Staff from The Lighthouse including those employed by, UCLH, Tavistock and Portman, NSPCC, Solace Women’s Aid, Camden Council and Met Police will be able to access the data and input data onto the Excelicare System.
      1. Each User will have access rights which may limit them from certain sensitive information.
         1. See Access Rights Form.

Excelicare system can only be accessed via the N3 network, using a NEL CSU laptop or other NHS laptop/computer.

* 1. Data will be shared with other Data Controllers/Disclosers and Data Processors/Retrievers as detailed below in this clause:
     1. Information regarding individual case management, physical health, mental health, criminal justice process and support will be shared within partners providing the Lighthouse through the Excelicare shared record as described in section 6
     2. Information regarding case management, safeguarding and summary findings will be shared with local partners including police, social worker, GP where:
        1. There is a safeguarding duty to share information for children or young people at risk
        2. Children and young people have consented to using the Lighthouse service with the full knowledge that we will share information where there is a safeguarding risk.
     3. The Lighthouse staff will share perpetrator themes and trends/location of incident with police liaison officers and Met Police intelligence department.
        1. Where themes and trends regarding perpetrators that are potential risk to community are identified in allocation meetings and weekly case review meetings, the Lighthouse will share those themes and trends with police intelligence department
        2. Where children, young people and parents/carers do not wish police to investigate, the Lighthouse will ensure they minimise risk of identify child/young person/family when themes and trends are reported
     4. The Lighthouse will provide an extract of data from Excelicare to MOPAC for evaluation. Data will only be extracted for children and young people that have explicitly given informed consent for personally identifiable data to be shared with MOPAC, as explained in the Evaluation Consent Form
        1. A data processing agreement is in place between UCLH and Excelicare
        2. MOPAC will not access Excelicare records directly to seek evaluation data
     5. Lighthouse delivery partners (UCLH, Tavistock and Portman, and NSPCC) agree to share monitoring and reporting of performance data related to services and staff from their organisations working in the Lighthouse including:
        1. Activity and referral data
        2. Service provision at evenings and weekends
        3. Operational efficiency such as caseloads, room use
        4. Case management, risk and outcomes data

1. Classification of Data
   1. All sensitive or personal identifiable data will be classified as OFFICIAL-SENSITIVE and will be accessed on a ‘need-to-know’ basis. Please refer to the NHS Digital Classification scheme for more information.
2. Consent
   1. Children and young people, and parents/carers as appropriate, will be provided with a privacy statement and the opportunity to agree to the service before any assessment, treatment or support is provided by the Lighthouse.
   2. We will only work with children and young people with their agreement and understanding of what information will be recorded and how we will keep this safe. Lighthouse workers will explain the process to the child, young person and their parent/carer and provide a privacy statement for them to review and sign.
   3. The privacy statement will explain that there will be times when we cannot keep information confidential. This means that if the child or young person, or another person, is at risk we might need to share this information with partner agencies.
   4. We will seek explicit informed consent for the child of young person’s data to be included in the MOPAC evaluation
   5. We will seek explicit informed consent for the child or young person to have a video recorded genital examination
   6. We will seek explicit informed consent for the child or young person to take part in the Forensic Interviewing Pilot
3. Lawful, fair and transparent processing
   1. Each party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with clause 8 during the Term of this agreement.
   2. The purpose of this Agreement is to allow the fulfilment of the service provided by The Lighthouse. The lawful processing condition that makes sharing legitimate under the Data Protection Legislations is Article 6 (1)(b) Processing is necessary for the performance of a contract to which the data subject is part or in order to take steps at the request of the data subject prior to entering into a contract.
   3. The Data Discloser shall, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the data subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required by Article 13 of the GDPR including:
      * 1. if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the data subject to understand the purpose and risks of such transfer; and
   4. The Data Receiver undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required by Article 14 of the GDPR including:
      * 1. if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the data subject to understand the purpose and risks of such transfer.
4. Data quality
   1. Shared Personal Data must be limited to the Personal Information described in [clause 8] of this Agreement.
   2. The Data Receiver/processor shall not delete or remove any other information that may be contained within or relating to the Shared Information.
   3. All parties shall take responsibility for preserving the integrity of the Shared Personal Information and preventing the corruption or loss of the Shared Personal Information of those receiving services within the Lighthouse.
5. Data subjects' rights
   1. The parties each agree to provide such assistance as is reasonably required to enable the Lighthouse Service Manager to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation. These will only relate to Subject Access Requests for any data held on the Excelicare system or records held by The Lighthouse.
   2. The PoC for UCLH are responsible for maintaining a record of individual subject access requests (SAR) for information for any data held on Excelicare. Records must include copies of the request for information and SAR application form, proof of identity, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The PoC for each party are detailed in clause 4.7.
   3. See the Lighthouse Subject Access Request guideline for the process.
6. Freedom of Information
   1. The Parties to this Agreement are subject to and shall comply with the provisions of the Freedom of Information Act 2000. This document and the arrangements it details will be disclosable for the purposes of the Freedom of Information Act 2000.
   2. Those Parties to this Agreement that are ‘public authorities’ for the purposes of the Freedom of Information Act 2000 may receive requests for information relating to the information sharing activities under this Agreement (e.g. statistics on the amount of data sharing being undertaken or the general nature of the data sharing). It is recognised that public authorities are individually responsible for meeting their obligations under the Freedom of Information Act 2000. Under the Section 45 of the Code of Practice on handling requests for information, good practice is to consult with third parties who have given information which may be disclosed under the Act. The Parties are therefore expected where they receive such requests to ensure that Parties to this Agreement are consulted in a suitable manner of the nature of the request and their intended response. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to information they do not hold. There will be an expectation that personal data requested by third parties will be exempted under section 40 Freedom of Information Act 2000.
   3. See the Freedom of Information Policy for more information.
7. Data retention and deletion
   1. The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. See Data Protection Policy for more information on retention.
   2. Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective industry.
   3. The time limit to ensure that the data is deleted will be agreed as 5 working days.
   4. In the event of the Lighthouse Pilot Scheme being dissolved after the initial two-year period, the Data Receiver shall ensure that any Shared Personal Information are returned to the Data Discloser, not later than one working day, after is ceases to be required in the following circumstances:
      1. on termination of the Agreement;
      2. on expiry of the Term of the Agreement;
      3. once processing of the Shared Personal Information is no longer necessary for the purposes it was originally shared for.
      4. Termination of the Lighthouse Pilot Scheme.
8. Transfers
   1. For the purposes of this clause, transfers of personal data shall mean any sharing of personal data by the Data Receiver with a third party, and shall include, but is not limited to, the following:
      1. subcontracting the processing of Shared Personal Data;
      2. granting a third-party controller access to the Shared Personal Data.
   2. The Data Receiver or Processor shall not disclose information to any third party without the prior written agreement of the Joint Data Controller(s), mainly the Lighthouse Service Manager.
   3. If the Data Receiver appoints a third-party processor to process the Shared Personal Information, it shall comply with Article 28 and Article 30 of the GDPR and shall remain liable to the Data Discloser for the acts and/or omissions of the processor.
   4. TheData Receiver shall not disclose or transfer Shared Personal Data outside the EEA.
   5. On termination of the pilot scheme, Excelicare will provide the data from their system to the relevant Data Owners and a recipient from each party will be provided. NEL CSU will provide UCLH with the information that will be held on the Lighthouse Shared Drive. UCLH will receive all of the Shared Drive Data and will then send on to specific partners. UCLH will ultimately own and keep the master archive copy.
      1. The service manager will work with partners and clarify who the data owner will be at the time of the transfer.
9. Security and training
   1. The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods as agreed in this agreement.
   2. The parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:
      1. prevent:
         1. unauthorised or unlawful processing of the Shared Personal Data; and
         2. the accidental loss or destruction of, or damage to, the Shared Personal Data
      2. ensure a level of security appropriate to:
         1. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
         2. the nature of the Shared Personal Data to be protected.
   3. The level of technical and organisational measures agreed by the parties as appropriate as at the Commencement Date having regard to the state of technological development and the cost of implementing such measures is set out in the Information Security Policy. The parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term.
   4. It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in Information Security Policy, together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the processing of personal data.
      1. IG training will be undertaken by staff at their employing trust or organisation as part of Statutory and Mandatory training
      2. Lighthouse IG awareness and training will be provided to all staff before Commencement date or during Lighthouse induction for staff joining after that time
   5. The level, content and regularity of training referred to in Clause 18.4 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the Shared Personal Data.
10. Personal data breaches and reporting procedures
    1. The parties shall each comply with its obligation to report a Personal Data Breach to the Lighthouse Service Manager and (where applicable) data subjects under Article 33 of the GDPR and shall each inform all relevant and required party of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or data subject(s).
    2. The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.
    3. Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of the relevant Partner.
11. Review and termination of agreement
    1. Any additional Data Receiver that wishes to be part of this data sharing initiative and Agreement shall complete and submit a written request. The consent of every party is required in order for the additional party to be included into this Agreement.
    2. In the event that a party terminates the Agreement or a new Data Receiver joins the agreement in accordance with clause 20.1, an amended and updated version of this Agreement will be drafted as soon as practicable and circulated to all other parties.
    3. Parties shall review the effectiveness of this data sharing initiative every twelve months and on the addition and removal of a party, having consideration to the aims and purposes set out in clause 4. The parties shall continue, amend or terminate the Agreement depending on the outcome of this review.
    4. The review of the effectiveness of the data sharing initiative will involve:
       1. assessing whether the purposes for which the Shared Personal Data is being processed as agreed in this Agreement;
       2. assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and
       3. assessing whether personal data breaches involving the Shared Personal Data have been handled in accordance with this Agreement and the applicable legal framework.
    5. Each party reserves its rights to inspect the other party's arrangements for the processing of Shared Personal Data and to terminate the Agreement where it considers that the other party is not processing the Shared Personal Data in accordance with this agreement.
12. Resolution of disputes with data subjects or the Supervisory Authority
    1. In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
    2. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
    3. Each party shall abide by a decision of a competent court of the Data Discloser's country of establishment or of the Supervisory Authority.
13. Language
    1. This Agreement is drafted in the English language. If this Agreement is translated into any other language, the English language version shall prevail.
    2. Any notice given under or in connection with this Agreement shall be in English. All other documents provided under or in connection with this Agreement shall be in English, or accompanied by a certified English translation.
    3. The English language version of this agreement and any notice or other document relating to this agreement shall prevail if there is a conflict except where the document is a constitutional, statutory or other official document.
14. Warranties
    1. Each party warrants and undertakes that it will:
       1. Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations.
       2. Make available on request to the data subjects who are third party beneficiaries a copy of this Agreement, unless the Clause contains confidential information.
       3. Respond within one working day and as far as reasonably possible to enquiries from the relevant Supervisory Authority in relation to the Shared Personal Data.
       4. Respond to Subject Access Requests in accordance with the Data Protection Legislation and Lighthouse Subject Access Request guideline.
       5. Work together to respond to Subject Access Requests and provide information within one working day to the other Party when this is requested to fulfil a Subject Access Request.
       6. Where applicable, maintain registration with all relevant Supervisory Authorities to process all Shared Personal Data for the Agreed Purpose.
       7. Take all appropriate steps to ensure compliance with the security measures set out in clause 18 above.
    2. The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Data to the Data Receiver and it will ensure that the Shared Personal Data are accurate.
    3. Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.
15. Indemnity
    1. The Data Discloser and Data Receiver undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Agreement, except to the extent that any such liability is excluded under clause 26.
    2. Indemnification hereunder is contingent upon
       1. the party(ies) to be indemnified (the indemnified party(ies)) promptly notifying the other party(ies) (the indemnifying party(ies)) of a claim,
       2. the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and
       3. the indemnified party(ies) providing reasonable co-operation and assistance to the indemnifying party(ies) in defence of such claim.
16. Allocation of cost

Each party shall perform its obligations under this Agreement at its own cost or where agreed the costs will be covered by The Lighthouse.

1. Limitation of liability
   1. No party(s) excludes or limits liability to the other party for:
      1. fraud or fraudulent misrepresentation;
      2. death or personal injury caused by negligence;
      3. a breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
      4. any matter for which it would be unlawful for the parties to exclude liability.
   2. Subject to clause 26.1, no party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:
      1. any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;
      2. loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or
      3. any loss or liability (whether direct or indirect) under or in relation to any other contract.
   3. Data Processing Agreement [Between The Lighthouse and Excelicare] shall not prevent claims, for:
      1. direct financial loss that are not excluded under any of the categories set out in clause 26.2(a); or
      2. tangible property or physical damage.
2. Third party rights
   1. Except as expressly provided in clause 14 (data subjects rights) and [or elsewhere in this Agreement], a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement. This does not affect any right or remedy of a third party which exists, or is available, apart from that Act.
   2. No one other than the parties to this Agreement, their successors and permitted assignees, shall have any right to enforce any of its terms. A data sharing agreement must be in place for the duration of the contract between the parties.
3. Variation

No variation of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

1. Waiver

No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

1. Severance
   1. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement.
   2. If any provision or part-provision of this agreement is deemed deleted under clause 30.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.
2. Changes to the applicable law

If during the Term the Data Protection Legislation changes in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the PoCs will negotiate in good faith to review the Agreement in the light of the new legislation.

1. No partnership or agency
   1. Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.
   2. Each party confirms it is acting on its own behalf and not for the benefit of any other person.
2. Entire agreement
   1. This Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
   2. Each party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.
   3. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misrepresentation based on any statement in this Agreement.
3. Further assurance

At its own expense, each party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this agreement.

1. Force majeure

No parties shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control.

1. Rights and remedies

Except as expressly provided in this Agreement the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

1. Notice
   1. Any notice or other communication given to a party under or in connection with this agreement shall be in writing, addressed to the PoCs and shall be:
      1. delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
      2. or sent by email to the PoC].
   2. Any notice or communication shall be deemed to have been received:
      1. if delivered by hand, on signature of a delivery receipt;
      2. if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting [or at the time recorded by the delivery service, and
      3. if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 35.2(c), business hours mean 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.
   3. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution
2. Governing law

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

1. Jurisdiction

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this Agreement or its subject matter or formation.

This agreement has been entered into on the date stated at the beginning of it.

1. Agreement Formalities

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Signed on behalf of……………………………………………..

Name (print)………………………………………………………

Role………………………………………………………………...

Signature………………………………………………………….

Date / /

Appendix A:

Lighthouse data sharing summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Organisation | Controller | Processor | Data discloser | Data receiver from Excelicare |
| UCLH | Yes |  | Staff enter data into Excelicare | Create reports in Excelicare including service level reports and dashboards  Where explicit consent given, quality assure the data extract created for evaluation by Axsys and data extract for research |
| T&P | Yes |  | Staff enter data into Excelicare | Receive service level reports |
| NSPCC | Yes |  | Staff enter data into Excelicare | Receive service level reports |
| MOPAC | Yes |  |  | Data extract with patient identifiable data for evaluation – only where explicit consent has been given by child, young person and/or family/carer |
| Excelicare |  | Yes |  | Host data on Excelicare server at RedCentric and create and run report templates for QAF, Evaluation, and dashboards |
| NEL CSU |  | Yes |  | Host Lighthouse shared drive on NEL CSU server in the Lighthouse |
| Met Police |  | Yes | Staff enter data into Excelicare | Receive service level reports |
| Camden Council |  |  | Staff enter data into Excelicare | Receive service level reports |
| Solace Women’s Aid |  |  | Staff enter data into Excelicare | Receive service level reports |