|  |  |
| --- | --- |
| Name of Policy | Data Protection Policy |
| Version Date | 16th October 2018 |
| Approved by | Nick Roberts, Director of Digital Services, UCLH |
| Date | 16th October 2018 |
| Review Date | October 2019 |
| Target Audience | Staff employed by UCLH, T&P, Met Police, NSPCC, London Borough of Camden, Solace and any other contractual staff employed on behalf of The Lighthouse. |
| Authored by | Ikram Musa |
|  |  |

­

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Owner** | **Changes Made** |
| 1.0 | 16/10/18 | Deborah Dillon |  |

|  |
| --- |
| The 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. |

**Table of Contents**

[**1.** **Introduction** 3](#_Toc527198981)

[**1.1.** **Policy scope** 3](#_Toc527198982)

[**1.2.** **Disclosure** 3](#_Toc527198983)

[**2.** **People, risks and responsibilities** 5](#_Toc527198984)

[**2.1.** **Data Subject** 5](#_Toc527198985)

[**2.2.** **Data Controller** 5](#_Toc527198986)

[**2.3.** **Data Processor** 5](#_Toc527198987)

[**2.4.** **Data collection** 5](#_Toc527198988)

[**2.5.** **Data Storage** 6](#_Toc527198989)

[**2.6.** **Data Use** 7](#_Toc527198990)

[**2.7.** **Data Accuracy** 7](#_Toc527198991)

[**2.8.** **Data Access** 7](#_Toc527198992)

[**2.9.** **General Employee Guidelines** 8](#_Toc527198993)

[**2.10.** **Subject Access Requests (SAR)** 8](#_Toc527198994)

[**2.11.** **Data protection risks** 9](#_Toc527198995)

[**2.12.** **Data Breach** 9](#_Toc527198996)

[**3.** **Providing Information** 10](#_Toc527198997)

[**Glossary of Terms** 11](#_Toc527198998)

# 

# **Introduction**

The Lighthouse needs to gather, store and process personal and/or sensitive information about the CYP or data subjects who attend 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 and the NSPCC) 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 justice, support and/or therapy services. This personal data must be processed appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there must be safeguards to ensure this under the Data Protection Act 2018. This policy describes how this personal data must be collected, handled and stored to meet The Lighthouse’s data protection standards — and to comply with the law.

## **Policy scope**

This policy applies to:

* The Lighthouse.
* All staff employed by University College London Hospital, The Tavistock and Portman NHS Foundation Trust, NSPCC, Met Police, London Borough of Camden and Solace working at The Lighthouse.
* All staff and volunteers of The Lighthouse.
* All volunteers, contractors, suppliers and other people working on behalf of University College London Hospital, The Tavistock and Portman NHS Foundation Trust and the NSPCC, Met Police, Social Care and Solace.

It applies to all data that The Lighthouse holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

* Names of individuals,
* Addresses,
* Email addresses,
* Telephone numbers,
* Sex/Gender,
* Age,
* Incident information,
* Treatment provided,
* Any other information relating to individuals.

## **Disclosure**

Personal Information collected at the Lighthouse may be shared with other agencies such asthe local authority, funding bodies and other voluntary agencies in order to provide a seamless service.

The child/young person (CYP) will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows The Lighthouse to disclose data (including sensitive data) without the data subject’s consent.

These are:

* Carrying out a legal duty or as authorised by the Government.
* Protecting vital interests of a CYP or another person.
* If the CYP has already made the information public.
* Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
* Monitoring for equal opportunities purposes – i.e. race, disability or religion.
* Providing a confidential service where the CYP’s consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill CYP to provide consent signatures.

The Lighthouse regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. The Lighthouse intends to ensure that personal information is treated lawfully and correctly. To this end, The Lighthouse will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 2018. Specifically, the Principles require that personal information:

* Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
* Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes.
* Shall be adequate, relevant and not excessive in relation to those purpose(s).
* Shall be accurate and, where necessary, kept up to date.
* Shall not be kept for longer than is necessary.
* Shall be processed in accordance with the rights of data subjects under the Act.
* Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.
* Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of CYPs/Service Users in relation to the processing of personal information.

The Lighthouse will, through appropriate management and strict application of criteria and controls**:**

* Observe fully conditions regarding the fair collection and use of information.
* Meet its legal obligations to specify the purposes for which information is used.
* Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements.
* Ensure the quality of information used.
* Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
  + The right to be informed that processing is being undertaken,
  + The right of access to one’s personal information,
  + The right to prevent processing in certain circumstances and
  + The right to correct, rectify, block or erase information which is regarded as wrong information).
* Take appropriate technical and organisational security measures to safeguard personal information.
* Ensure that personal information is not transferred abroad without suitable safeguards.
* Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
* Set out clear procedures for responding to requests for information.

# **People, risks and responsibilities**

## **Data Subject**

A data subject is any person whose personal data is being collected, held or processed. In this case, a data subject can be an employee, a child/young person who seeks help from the Lighthouse, suppliers, contractors and any employee from University College London Hospital, The Tavistock and Portman NHS Foundation Trust, the NSPCC, Solace, Met Police or Social Care.

## **Data Controller**

University College London Hospital, The Tavistock and Portman NHS Foundation Trust and the NSPCC are the providers of the Lighthouse service and joint Data Controllers under the Act, which means that they determine what purposes personal information held, will be used for. It is also their responsible for notifying the Information Commissioner of the data they hold or is likely to hold, and the general purposes that this data will be used for.

MOPAC are also joint data controllers through their role in commissioning the Excelicare data system, as the overall lead for the programme and as the lead for the evaluation.

Being a data controller does not mean that any organisation can have full access to all the data collected by the service without having due regard to the broader principles of GDPR. MOPAC has agreed that it will **not** have direct access to the data on Excelicare and that this will be provided by the UCLH team via an extract from the Excelicare system.

All parties have agreed that the lawful basis for sharing of evaluation data will be explicit consent. MOPAC will work with the Lighthouse team to further define the precise dataset that will be used for the evaluation. This will include personally identifiable data only where consent has been given. Only data where explicit consent has been given will be shared with MOPAC (this excludes aggregate level data that will be shared for contract management purposes which will be fully enable provided by the Lighthouse team to MOPAC and NHSE London).

The Lighthouse will use the privacy statement and allow advocate time to allow child/young/family to fully consider explicit consent.

## **Data Processor**

Excelicare and NEL CSU will be classed Data Processors under the Act, who will be processing the data on behalf of the data controller. Excelicare will be providing the software solution and the server for storing case management system data. NEL CSU will be providing the infrastructure, network, kit and server on which the Lighthouse shared drive data will be kept and stored on.

Solace are sub-contractors on behalf of NSPCC and are advocates providing advocacy services. As they will be working on the Lighthouse, they will be processing data onto the Excelicare system.

Met Police and London Borough of Camden Social Care employ the police liaison officers and social care liaison officers that work in the Lighthouse and will be processing data onto the Excelicare system.

## **Data collection**

Lighthouse will make sure that:

* A Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.
* At a later part of the process we will ask for consent to pass personal information to MOPAC to undertake the evaluation of the service that has been provided.

Service users will still have the option to withdraw their consent whenever they wish to do so.

The Lighthouse will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, The Lighthouse will ensure that the CYP:

1. Clearly understands why the information is needed.
2. Understands what it will be used for and what the consequences are should the CYP decide not to give agreement to processing.
3. As far as reasonably possible, gives agreement, either written or verbal for data to be processed.
4. Is, as far as reasonably practicable, competent enough to give agreement and has given so freely without any duress.
5. Has received sufficient information on why their data is needed and how it will be used.

## **Data Storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Lighthouse Service Manager.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

* Any data/information captured as notes/minutes/check-up information, will be scanned and uploaded onto Excelicare.
* When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
* Lighthouse staff should make sure that paper and printouts are **not left where unauthorised people could see them**, like on a printer.
* **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

* Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
* If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
* Data should only be stored on **The Lighthouse drives and allocated servers**, and should only be uploaded to the approved system.
* Servers containing personal data should be **sited in a secure location**, away from general office space.

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and contractors.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

## **Data Use**

When personal data is accessed and used there can be at the greatest risk of loss, corruption or theft:

* When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
* Personal data **should not be shared informally**.
* Data must be **encrypted before being transferred electronically**. Guidelines can be provided to explain how to send data to authorised external contacts.
  + All Lighthouse staff will be provided with an NHS Email Address and any data (if required) must be transferred using NHSmail or GCSX.
* Personal data should **never be transferred outside of the European Economic Area**.
* Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

## **Data Accuracy**

The law requires all staff within The Lighthouse to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional datasets and ensure that the data held on the Excelicare system is kept up to date and classed as ‘complete data.
* Staff should **take every opportunity to ensure data is updated.** For instance, by confirming CYP’s address is still the same when they visit The Lighthouse Facility.
* The Lighthouse will make it **easy for data subjects to update the information** TheLighthouse holds about them via the Excelicare system.
* Data should be **updated as inaccuracies are discovered**. For instance, if a CYP can no longer be reached on their stored telephone number, it should be removed from Excelicare or any records.

## **Data Access**

The Lighthouse will ensure that data is managed by following good Data Protection Practice, in addition to:

* Everyone processing personal information understands that they are contractually responsible for following good data protection practice
* Everyone processing personal information is appropriately trained to do so
* Everyone processing personal information is appropriately supervised
* Anybody wanting to make enquiries about handling personal information knows what to do
* It deals promptly and courteously with any enquiries about handling personal information
* It describes clearly how it handles personal information
* It will regularly review and audit the ways it holds, manage and use personal information
* It regularly assesses and evaluates its methods and performance in relation to handling personal information

All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

In case of any queries or questions in relation to this policy please contact The UCLH Protection Officer. As UCLH are the lead provider for health and wellbeing services in the Lighthouse, the UCLH DPO will respond back to any queries. They can be contacted via [UCLH.IGQueries@NHS.net](mailto:UCLH.IGQueries@NHS.net).

## **General Employee Guidelines**

* The only people able to access data covered by this policy should be those who **need it for their work**.
* Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers or from the data owners.
* **The Lighthouse will provide training** to all staff to help them understand their responsibilities when handling data.
* Staff should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, **strong passwords must be used** and they should never be shared.
* Personal data **should not be disclosed** to unauthorised people, either within The Lighthouse or externally.
* Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
* Staff **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

## **Subject Access Requests (SAR)**

All service users who are the subject of personal data held by The Lighthouse are entitled to:

* Ask **what information** The Lighthouse holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how The Lighthouse is **meeting its data protection obligations**.

If a service user contacts The Lighthouse requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to a single point of contact for the joint data controllers at [UCLH.thelighthouse@NHS.net](mailto:UCLH.thelighthouse@NHS.net). The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for the subject access request unless the request is manifestly unfounded or excessive, the requester may be charged a reasonable fee which will be clarified once the request has been analysed. The fee may also be applied fee if an individual requests further copies of their data following a request and the fee will be based on the administrative costs of providing further copies.

The data controller will aim to provide the relevant data within 30 days. All requests must be dealt without undue delay and at the latest within one month of receipt. This will be calculated from the day after the request has been received (whether the day after is a working day or not) until the corresponding calendar data in the next month.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

These requests will be logged in an Excel spreadsheet as a Tracker and will updated as the request is processed.

See Subject Access Request Guidelines for further information.

## **Data protection risks**

This policy helps to protect The Lighthouse from some very real data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Failing to offer choice.** For instance, all children/young people should be free to choose how The lighthouse uses data relating to them
* **Reputational damage.** For instance, The lighthouse could suffer if hackers successfully gained access to sensitive data or if the sensitive data is leaked

## **Data Breach**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

It is each stakeholder’s duty to report certain types of personal data breach to the relevant supervisory authority. This must be done this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting CYP’s rights and freedoms, you must also inform The UCLH Data Protection Officer who should contact the CYP without undue delay.

Examples of data breaches (but not limited to):

* Cybercrime Hacking
  + External hacker accesses data held on Excelicare or gets hold of sensitive data held on paper.
  + Phishing attack via email/telephone.
* Loss or Theft of Mobile Device or Media
  + Contains sensitive patient data, resulting in potential unauthorized access to that data.
* Insider Accidents or Workarounds
  + Well-intentioned action that results in unauthorised access to sensitive patient information.
    - For example, emailing unsecured sensitive patient information, resulting in potential unauthorised access to this information.
* Data Processor Incident
  + A third-party organisation i.e. Excelicare contracted by The Lighthouse experiences a breach event involving unauthorised access to sensitive patient information.
* Malicious Insiders or Fraud
  + A worker performs a malicious action that results in unauthorised access to sensitive patient information.
    - Prescription Fraud,
    - Financial Fraud,
    - Medical Claims Fraud – Selling patient data.
* Insider Snooping
  + A worker accessing the records of patients of your organisation without any legitimate need to do so, for example where a patient is not under the direct care of the worker.
* Subject access
  + Acknowledgement are not sent within a reasonable time,
  + SAR are not met within 30 days.
* Datix reports
  + Incident reports are not completed or submitted,
  + Reports are not queried or actioned/completed.
* Data Protection Act 2018
  + Good practice through processes and procedures are not followed to ensure compliancy.

In case of any queries or questions in relation to this policy please contact The Lighthouse Data Protection Officer: Deborah Dillon. As UCLH are the lead trust entrusted on the Lighthouse, the UCLH DPO will respond back to any queries. They can be contacted via [UCLH.IGQueries@NHS.net](mailto:UCLH.IGQueries@NHS.net).

# **Providing Information**

The Lighthouse aims to ensure that service users are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, The Lighthouse has a privacy notice as part of this policy, setting out how data relating to CYP is used by The Lighthouse.

# **Glossary of Terms**

**Data Controller** – The person who (either alone or with others) decides what personal information The Lighthouse will hold and how it will be held or used.

**Data Protection Act 1998** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**Data Protection Officer** – The person(s) responsible for ensuring that The Lighthouse follows its data protection policy and complies with the Data Protection Act 1998.

**CYP/Service User** – The person whose personal information is being held or processed by The Lighthouse for example: a client, an employee, or supporter.

**Explicit consent** – is a freely given, specific and informed agreement by an CYP/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

**Notification** – Notifying the Information Commissioner about the data processing activities of The Lighthouse, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self-assessment guide will help you to decide if you are exempt from notification: <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx>

**Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

**Processing** – means collecting, amending, handling, storing or disclosing personal information.

**Personal Information** – Information about living CYPs that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as CYP volunteers or employees within (GROUP).

**Sensitive data** – refers to data about:

* Racial or ethnic origin
* Political affiliations
* Religion or similar beliefs
* Physical or mental health
* Sexuality
* Criminal record or proceedings