Data Protection Policy

Thorpe House Specialist Adult Mental Health Unit Ltd (THSAMHU), uses and stores personal information about our colleagues (this includes employees, directors, trustees, consultants, contractors and potential employees)
THSAMHUL also receives, uses and stores personal information about our service users, their next of kin and their emergency contacts.
THSAMHUL receives, uses and stores personal information of health professionals involved in our service users care.
THSAMHUL must handle that information lawfully, in line with the requirements of the *Data Protection Act 2018* and the General Data Protection Regulation, to maintain trust between the Company and the individual.

This policy sets out the basis on which we will process any personal data we collect.

Tobias Knight (Director) is responsible for ensuring compliance with relevant data protection legislation and with this policy. Any queries or concerns regarding the implementation of this policy should be referred in the first instance to James Lockwood (Nursing Manager).

What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special category data includes sensitive personal data about a person's racial or ethnic origin, political opinions, religious, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and 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.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Fair and Lawful Processing

THSAMHUL will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Processing for Limited Purposes

THSAMHUL will only process personal data for purposes permitted by the Data Protection legislation; unless in a medical emergency. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notifying Individuals and their rights

If we collect personal data directly from an individual, we will process it in line with their rights and we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The types of third parties, if any, with which we will share or disclose that personal data.
d. Any personal data that is intended to be transferred to a non-European Economic Area country or international organisation and that the appropriate and suitable safeguards in place.
e. How individuals can limit our use and disclosure of their personal data.
f. Information about the period that their information will be stored, or the criteria used to determine that period.
g. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h. Their right to object to processing and their right to data portability.
i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. The right to lodge a complaint with the Information Commissioners Office.
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual and their right not to be subject to this in certain circumstances.
n. That we are the data controller and provide contact details to enable individuals to exercise their rights and/or raise a complaint.

This notification will usually take the form of a privacy notice.

Adequate, Relevant and Non-excessive Processing

THSAMHUL will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data

THSAMHUL will ensure that personal data we hold is accurate and kept up to date. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing

THSAMHUL will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Data Security

THSAMHUL will take appropriate organisational and security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to external data processors if they agree to comply with those procedures and policies, or that they put in place adequate measures themselves.

We will raise awareness of data protection legislation and regulations and train our staff on data protection policies and procedures to maintain security of personal data.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data as set out in our Information Security Policy.

If we transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organisation, we will ensure one of the following conditions applies:

a. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
b. The data subject has given his consent.
c. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
d. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
e. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work with one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, and the provision of support services.

Disclosure and Sharing of Personal Data

THSAMHUL may share employee personal data with a number of third parties in order to fulfil the terms and conditions of employment including provision of payroll and benefits, these include:

- Training Providers
- Pension Scheme Administrators

- HR and Legal Advisors
- Benefit providers (e.g. childcare vouchers, cyclescheme, healthcare provider)

A list of current providers of these services is available on request from Tobias Knight.

We may be required to share personal information to comply with legal, statutory and regulatory obligations, where there is evidence of criminal activity (including fraud) or where there is a material health and safety risk.

Outside of this, disclosure outside of the organisation of personal data will only be made with explicit and informed consent of the individual and where there is a compliant data sharing agreement in place.

Subject Access Requests

Individuals can make a formal request for information we hold about them to Tobias Knight (Director). Employees who receive a request should forward it to Tobias Knight (Director) immediately, who will coordinate the response.

Where an individual has requested access to their personal data, one copy will be provided free of charge (unless the request can be evidenced to be manifestly unfounded or excessive) within one month of receipt of the request.

Where a request has been made electronically, data will be provided in a commonly-used electronic form unless the individual has requested otherwise.

Data will be withheld if it adversely affects the rights and freedoms of others.

APPENDIX B BREACH MANAGEMENT PROCEDURE

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

1. Identification and reporting

All potential and actual breaches must be reported immediately to Tobias Knight (Director). In the absence of Tobias Knight, a member of THSAMHUL Board should be notified.

2. Containment and Damage Limitation.

On discovery of the breach Tobias Knight (Director) in conjunction with relevant staff members will investigate the cause of the breach and consider what immediate measures can be taken to recover the data and/or ensure damage limitation e.g. changing passwords, remote phone wipe.

3. Assessing the risks

Tobias Knight (Director) will consider the consequences of the breach both for the organisation and data subjects concerned.

4. Notification of breaches

Tobias Knight (Director) will consider who it is necessary to notify regarding the breach (e.g. the data subject) and check whether a formal disclosure to the Information Commissioner is required (i.e. where it is likely to result in a risk to the rights and freedoms of individuals and a significant detrimental effect on them). If the breach is considered severe, the THSAMHUL Board of Directors may need to be notified.

Where appropriate notification to the Information Commissioner must be done within 72 hours of the Company becoming aware of it. The notification must contain the following information:

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

It will often be impossible to investigate a breach fully within that time-period and allows this information to be provided in phases with the agreement of the Information Commissioner. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

The Information Commissioner can provide guidance as to whether and how individuals should be notified if it is not immediately clear.

Where the breach concerns data that the Company is processing on behalf of another organisation, that organisation must be notified immediately as detailed in the relevant Data Sharing Agreement.

5. Evaluation and response

A register of personal data breaches and actions taken will be maintained by Tobias Knight (Director) and reported to the THSAMHUL Board of Directors on an annual basis. This will include an analysis of the impact and causes of the breach and evaluate the effectiveness of the response, including an assessment of whether current policies and procedures are adequate.