General Data Protection Regulations Policy

DOCUMENT DETAILS	
Policy number:	LG05w (for website)
Version:	1.0
Target Audience (s):	☑ All Staff ☐Clinical Staff ☐Non Clinical Staff ☑External suppliers or visitors ☑Regulatory / Legal bodies ☑Other (eg. Patients)
Policy Author (Subject Matter Expert):	Fusion Law
Policy Committee Sponsor:	Peter Curtis
Frequency of review:	1 year
Last review date:	25/06/2018
Committee Ratification Date	25/06/2018
Next scheduled review date:	25/06/2019
Ellern Mede service (s) to which Policy applies:	☑Ellern Mede Ridgeway ☑Ellern Mede Barnet ☑Ellern Mede Outpatient

DOCUMENT HISTORY/CHANGE CONTROL			
Version number	Section Number	Date of change	Reason for change

TABLE OF CONTENTS

Definitions

For the purposes of this Policy and as provided for by the GDPR:

Automated Decision Making	means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Biometric Data	means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or data relating to finger print analysis;
Board	means the Board of Directors of the Company from time to time;
Business Purposes	means the purposes for which Personal Data may be used by the Company, e.g. service provision, personnel, administrative, financial, regulatory, payroll and business development purposes;
Company's Computer Systems	means all computer and other technological systems used by the Company during the normal course of its business and for the purpose of controlling and purposing the Personal Data of the Data Subject. The Company's Computer Systems shall contain up-to-date anti-virus and anti-malware software at all times and shall be fully secure and encrypted;
Consent	where the Company relies on consent as the lawful basis, the consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be

	provided for by Union or Member State law. The Data Controller is therefore a person or body who determines the purposes for which and the manner in which the Personal Data is to be used and Processed by the Data Processor;
Data Concerning Health	means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
Data Processor	means a natural or legal person, public authority, agency or other body which processes and uses Personal Data on behalf of the Controller. The Data Processor does not necessarily own or control the Personal Data but they will be involved in the use and Processing of the Personal Data on behalf of the Data Controller;
Data Protection Officer	Means the natural or legal person appointed to have formal responsibility for data protection compliance within the organisation. The Data Protection Officer ('DPO') has a sufficiently senior role to carry out the role of the DPO for the business and has sufficient independence to ensure that there is no conflict of interest.
EEA	means the European Economic Area which currently includes the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Enterprise	means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
Filing System	means any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
GDPR	means the General Data Protection Regulation ((EU) 2016/679).
Genetic Data	means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
Group of Undertakings	means a controlling undertaking and its controlled undertakings;
International Organisation	means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
Personal Data	means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

	physiological, genetic, mental, economic, cultural or social identity of that natural person. For the purposes of this Policy, Personal Data shall also include Sensitive Personal Data as defined in this Policy. The types of Personal Data and Sensitive Personal Data has been listed in Paragraph 2 of this Policy;
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 transmitted, stored or otherwise processed;
Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Profiling	means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
Pseudonymisation	means the anonymising of Personal Data through the use of a patient identification number rather than using and processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person;
Recipient	means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities, including but not limited to, the National Health Service (NHS), Care Quality Commission (CQC), Department of Justice and Department of Health, which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
Representative	means a natural or legal person established in the Union who, designated by the Controller or Processor in writing pursuant

	to Article 27, represents the Controller or Processor with regard to their respective obligations under this Regulation;
Restriction of processing	means the marking of stored Personal Data with the aim of limiting their processing in the future;
Supervisory Authority	means an independent public authority which is established by a Member State pursuant to Article 51. For the purposes of Companies incorporated in England and Wales the Supervisory Authority is the Information Commissioner's Office ('ICO');
Third Party	means a natural or legal person, public authority, agency or body, including but not limited to the National Health Service and external professionals of the Company, other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data;

GENERAL DATA PROTECTION REGULATIONS POLICY

1. INTRODUCTION

1.1 This Policy sets out the obligations of Oak Tree Forest Limited t/a Ellern Mede ("the Company") regarding data protection and the rights of Company's website (https://ellernmede.org/), and employees, independent contractors, agency workers, clients, customers, business contacts, suppliers and individuals for a variety of business purposes ("Data Subjects") in respect of their Personal Data under the General Data Protection Regulation (EU) 2016/679 ("the Regulation").

1.2 This policy sets out the collection, use, retention, transfer, disclosure and destruction of Personal Data regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject. The Policy seeks to protect Personal Data and ensure that staff understand the rules governing their use of Personal Data to which they have access in the course of their work.

1.3 The Company is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Please contact the Data Protection Officer, DPO, Mr Daniel Muscalu who may be contacted via email on Daniel.Muscalu@ellernmede.org, with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed.

2. DATA COVERED BY THE GDPR

2.1 The GDPR defines Personal Data as including:

1. Personal details;
2. Family and lifestyle details;
3. Education and training;
4. Medical details including biometric data;
5. Employment details;
6. Financial details;
7. Contractual details (for example, goods and services provided to a Data Subject);
8. Location data; and
9. Online identifiers e.g. IP addresses, cookie IDs, device identifiers etc.

2.2 The GDPR defines Sensitive Personal Data as Personal Data revealing:

1. Racial or ethnic origin;
2. Political opinions;
3. Religious and philosophical beliefs;
4. Trade- union membership;
5. Data concerning health or sex life and sexual orientation; and
6. Genetic data or biometric data.

For the purposes of this policy, Sensitive Personal Data is to be included within the definition of 'Personal Data'

3. The Data Protection Principles

3.1 This Policy aims to ensure compliance with the Regulation. This Policy aims to set out the best practice of the Company in relation to complying with the Regulation and ensuring that Personal Data is protected. The Regulation sets out the following principles with which the Company shall comply. All Personal Data shall be:

1. processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;
2. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
5. kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the Data Subject; and
6. 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.

4. Lawful, Fair and Transparent Data Processing

4.1 The Regulation seeks to ensure that Personal Data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject. The Regulation states that processing of Personal Data shall be lawful if at least one of the following applies:

1. the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the Controller is subject;
4. processing is necessary to protect the vital interests of the Data Subject or of another natural person;
5. 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; and
6. processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

Given the nature of the Company and the services we provide to our patients, including providing care and treatment for patients with eating disorders, the processing of Personal Data falls under Article 9(h) of the GDPR such that 'the processing is necessary for…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'. However, if for any reason Article 9(h) does not apply for the processing of Personal Data we shall ensure we have a lawful basis to process such data in accordance with this Paragraph 5 and 9.

5. Processed for Specified, Explicit and Legitimate Purpose

5.1 The Company collects and processes the Personal Data set out in Schedule 1 of this Policy. This may include Personal Data received directly from Data Subjects (for example, contact details used when a Data Subject

communicates with us) and data received from third parties (for example, general practitioner's, healthcare providers and family members, parents or guardians of the Data Subject).

5.2 The Company only processes Personal Data for the specific purposes set out in Schedule 4 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process Personal Data will be informed to Data Subjects or their parent and/or legal guardian at the time that their Personal Data is collected, where it is collected directly from the Data Subject, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

6. Accountability

6.1 The Company's Data Protection Officer is Mr Daniel Muscalu who may be contacted via email on daniel.muscalu@ellernemede.org or by telephone on 07470 755084.

6.2 The Data Protection Officer is responsible for:

1. Informing and advising the Company and our employees about their obligations to comply with the GDPR and other data protection laws;
2. Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
3. Acting as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)**;**
4. Completing internal audits of processing activities;
5. Providing training for all staff members who handle Personal Data and ensure access to further guidance and support;
6. Providing clear lines of report and supervision for compliance with data protection;
7. Carrying out regular checks to monitor and assess new processing of Personal Data and to ensure that any notification to the ICO is updated to take account of any changes in processing of Personal Data;
8. Developing and maintaining GDPR procedures;

6.3 The Data Protection Officer shall report to Mr Peter Curtis.

6.4 The Company confirms that the Data Protection Officer operates independently, and adequate resources have been provided to enable DPOs to meet their GDPR obligations.

6.5 All employees will, through appropriate training and responsible management:

1. Observe all forms of guidance, codes of practice and procedures about the collection and use of Personal Data;
2. Understand fully the purposes for which the Company uses Personal Data;
3. Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the Company to meet its service needs or legal requirements;
4. Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required;
5. On receipt of a request by or on behalf of an individual for information held about them will immediately notify their line manager; and
6. Not send any Personal Data outside of the United Kingdom without the authority of the Data Protection Officer.

6.6 The Company reserves its right to outsource the role of the Data Protection Officer to a third party that has thorough knowledge of the GDPR.

6.7 The Company shall keep written internal records of all Personal Data collection, holding, and processing, which shall incorporate the following information:

1. The name and details of the Company, its Data Protection Officer, and any applicable third- party data Controllers;
2. The purposes for which the Company processes Personal Data;
3. Details of the categories of Personal Data collected, held, and processed by the Company; and the categories of Data Subject to which that Personal Data relates;
4. Details (and categories) of any third parties that will receive Personal Data from the Company;
5. Details of any transfers of Personal Data to non-EEA countries including all mechanisms and security safeguards;
6. Details of how long Personal Data will be retained by the Company; and
7. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data

6.8 The Company shall also implement measures that meet the principles of data protection by design and data protection by default. Measures could include:

1. Data minimisation;
2. Ensuring transparency to Data Subjects and any relevant third parties follows consent obtained from Data Subjects;
3. Allowing Data Subjects to monitor processing;
4. Creating and improving security features on an ongoing basis; and
5. Use Data Protection Impact Assessments where appropriate as defined under paragraphs 12 and 17 of this Policy.

7. Consent

7.1 Where consent is the lawful basis relied upon, the consent obtained from a Data Subject shall not be valid unless separate consents are obtained for different processing activities. Forced, or 'omnibus', consent mechanisms will not be valid.

7.2 The Company recognises that the Data Subject has the right to withdraw consent at any time and may do so at any time by contacting the Data Protection Officer. If the Data Subject withdraws their consent, we shall make a record of this and ensure that Data Processing is stopped without undue delay and in any event within one month of the initial request.

7.3 We will also ensure that if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented we shall obtain separate and specific consent for the additional purposes.

7.4 When obtaining consent from a Data Subject the Company shall ensure:

1. The Data Subject has genuine choice and control – consent may not be valid if there is a clear imbalance of power;
2. Consent is not tied to a contract;
3. The Data Subject provides a positive opt-in. The company does not use pre-ticked boxes or any other method of consent by default; and
4. Explicit consent is acquired from the Data Subject for the use of Personal Data and the Data Subject is required to provide a very clear and specific statement that they consent to such use.

7.5 We provide the Data Subject with specific and granular options to consent to the different types of processing where appropriate. We do not provide the option for Data Subjects to provide blanket consent.

7.6 To ensure that the Data Subject's consent is properly and clearly obtained, we have ensured that our consent requests are kept separate from all other terms and conditions.

7.7 All requests for consent are in an intelligible and accessible form in clear and plain language.

7.8 The Company shall:

1. Name any third parties who will rely on the consent;
2. Make it easy for people to withdraw consent and tell them how;
3. Keep records and evidence of consent: who, when, how, and what you told people;
4. Keep consent under review, and refresh it if anything changes; and
5. Avoid making consent a precondition of a service.

8. Sensitive personal data

8.1 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

8.2 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

8.3

1. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
2. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
3. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
4. The processing relates to personal data which is clearly made public by the data subject;
5. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
6. The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
7. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
8. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard

the rights and freedoms of the data subject (in particular, professional secrecy); or

9. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Given the nature of the Company and the services we provide to our patients, including providing care and treatment for patients with eating disorders, the processing of Sensitive Personal Data falls under Article 9(h) of the GDPR such that 'the processing is necessary for…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'. However, if for any reason Article 9(h) of the GDPR does not apply for the processing of Personal Data we shall ensure we have a lawful basis to process such data in accordance with this Paragraph 8.

9. Specified, Explicit, and Legitimate Purposes

9.1 The Company collects and processes the personal data set out in Schedule 1 of this Policy. This includes:

1. 1. Personal data collected directly from data subjects; and
2. Personal data obtained from third parties.

9.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Schedule 1 of this Policy (or for other purposes expressly permitted by the GDPR).

9.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 18 for more information on keeping data subjects informed.

10. Children

10.1 The Company notes that children under the age of 13 can never, themselves, give consent to the processing of their Personal Data in relation to online services.

10.2 Therefore, and in accordance with our Capacity, Competency and Consent to Treatment Policy but except in the cases of preventative or counselling services to a child, we shall obtain parental consent before seeking to process Personal Data relating to children between the ages of 13 and 15 (inclusive). The Company shall use reasonable efforts to verify such parental consent, making use of available technology. For more information on matters relating to capacity and consent to treatment, please refer to our Capacity, Competency and Consent to Treatment policy, a copy of which is available on request from the Data Protection Officer.

10.3 Children aged 16 or older may give consent for the processing of their Personal Data themselves.

11. Privacy Notices

11.1 The Company will always inform a Data Subject about what we are doing with their Personal Data. This is to ensure that the Data Subject validly consents to our use of their Personal Data, to ensure the individual exercises their rights or, decide whether or not to provide us with their Personal Data.

11.2 The Company shall provide the Data Subject with a summary of unusual or important use of their Personal Data.

11.3 If requested by the Data Subject, the company shall provide a full privacy policy to the Data Subject within a reasonable time of the request including details of:

1. Sufficient information to identify our Company including our registered company name, company number and registered address as at Companies House;
2. Our contact details;
3. The contact details of any representative;
4. The contact details of Data Protection Officer;
5. The purpose and legal basis of any processing;
6. Details relating to the Data Subject's right to withdraw consent;
7. Categories of Personal Data processed;
8. Receipts or categories of recipients of Personal Data;

9. Details of any intended transfer outside of the EU and details of any safeguards relied upon;
10. The period for which data will be stored;
11. A list of the Data Subject's rights, including the right to object to direct marketing, make a Subject Access Request pursuant to paragraph 20 of this Policy and to be forgotten;
12. Details of any automated decision making as defined under paragraph 24 and consequences for the individual;
13. Whether provision of Personal Data is a statutory or contractual requirement, whether disclosure is mandatory and the consequences of not doing so; and
14. The individual's right to complain to a supervisory authority.

11.4 Where the data has been obtained directly from the Data Subject, the information stated under paragraph 11.3 shall be provided by the Company to the Data Subject at the time the data is obtained.

11.5 Where the data has not been obtained directly from the Data Subject, the information stated under paragraph 8.3 shall be provided by the Company to the Data Subject:

1. Within a reasonable period of the Company obtaining the data and, in any case, no later than one month after obtaining the data; or
2. If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
3. If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

12. Pseudonymisation

12.1 The Company shall ensure that Personal Data shall be processed in such a way that it can no longer be attributed to a specific Data Subject without the use of additional information.

12.2 Any identifying information shall be kept separately and be subject to technical and organisational measures to ensure non-attribution and to prevent inadvertent re-identification of the coded data such as hashing, encryption and coded data.

12.3 All Personal Data collected, processed and transferred by the Company shall be in a pseudonymised form.

12.4 We shall perform a Data Protection Impact Assessment (DPIA) before carrying out any processing that uses new technologies (taking into account the nature, scope, context and purpose of the processing) that is likely to result in a high risk to Data Subjects. The purpose of the DPIA is to act as an assessment to identify and minimise non-compliance risks.

12.5 A new DPIA shall be completed where there are new:

1. systematic and extensive processing activities, including profiling and where decisions have legal effects – or similarly significant effects – on individuals;
2. large scale processing of sensitive data or criminal convictions or offence details; or
3. large scale, systematic monitoring of public areas (CCTV).

12.6 If a DPIA is necessary, the Company shall consult with the Supervisory Authority prior to any processing taking place.

12.7 The Company has an ongoing requirement to keep all measures up to date including in the event of any new technology, product or service that involves the processing of Personal Data.

13. Adequate, Relevant and Limited Data Processing

13.1 The Company will only collect and process Personal Data for and to the extent necessary for the specific purpose(s) informed to Data Subjects.

13.2 The Company shall not retain any data which, in the Company's reasonable opinion, is irrelevant or excessive to the purposes for which the data was collected.

13.3 The Company shall ensure that the Personal Data shall be confidential by ensuring that only those who are required to have access to the Personal Data and who are authorised to use the Personal Data have access to it.

14. Accuracy of Data and Keeping Data Up To Date

14.1 The Company shall ensure and take reasonable steps to ensure that Personal Data collected and processed or that information provided by the individual concerned, or by another individual or organisation has been recorded correctly by the Company.

14.2 The Company shall also ensure that all Personal Data collected and processed is kept up- to- date where appropriate and as required under the GDPR.

14.3 The accuracy of data shall be checked when it is collected and at regular intervals thereafter.

14.4 Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. This is particularly important in relation to our patient records, medical records and details of next of kin. We shall, therefore, regularly check and confirm that these details are correct and amend any errors or omissions without undue delay.

14.5 However, the Company shall keep a record of the inaccuracy for transparency and clarity purposes provided these records are clear on the facts.

14.6 The Company shall ensure that the source of any Personal Data collected is clear and that clear records of such sources are maintained at all times.

14.7 Pursuant to the GDPR, accurate data means data which is correct and not misleading.

15. Timely Processing

15.1 The Company shall comply with its regulatory authorities, including but not limited to, the Care Quality Commission (CQC), in relation to retention periods for patient data and medical records. Nevertheless, the Company shall not keep Personal Data for any longer than is necessary in light of the purposes for which that data was originally collected and processed.

15.2 The Company shall store any hard copies of any Personal Data and Sensitive Personal Data at its premises at Ellern Mede Ridgeway, Holcombe Hill, the Ridgeway, Mill Hill, London, NW7 4HX no longer than necessary.

15.3 Electronic copies of any Personal Data or Sensitive Personal Data held by the Company shall be stored and downloaded by the Company using a secure server. The Company shall immediately delete any electronically downloaded folders when they are no longer required by the Company.

15.4 When the data is no longer required, all reasonable steps will be taken to securely erase it without delay.

15.5 The Company shall regularly review the Personal Data we hold and delete anything we no longer need.

15.6 If, in the Company's reasonable opinion the data will be required at a later date, the Company may archive the data (rather than delete it).

15.7 Any scanned copies of the personal data shall only be retained on the Company's Computer Systems for the purposes and duration for which they are required by the Company and in any event, shall be deleted from the Company's Computer Systems within three weeks from the date of scan.

16. Secure Processing

16.1 The Company shall ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Schedule 5 of this Policy.

16.2 The Company shall obtain an appropriate cyber security insurance policy in the event that there is an issue relating to a data breach.

16.3 Any electronic copies, including scanned copies, of any Personal Data will be held on the Company's Computer Systems. The Company's Computer Systems will have a username and password system for access. The passwords for the Company's Computer Systems will be changed every 3 months. The Company will ensure that it has up-to-date anti-virus and anti-malware software on its computer systems. Any electronic copies of any Personal Data that is held on the Company's computer systems will be encrypted and password protected, in addition to this Personal Data is to be pseudonymised.

16.4 If the Company keeps a guest sign in book when visitors visit the Company's premises, the Company shall ensure that appropriate measures are taken to keep the visitors details confidential and not disclose this to other visitors who are signing in.

17. Data Privacy Impact Assessments

17.1 The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's Data Protection Officer and shall address the following areas of importance:

1. purpose(s) for which Personal Data is being processed and the processing operations to be carried out on that data;
2. Details of the legitimate interests being pursued by the Company;
3. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
4. An assessment of the risks posed to individual Data Subjects; and
5. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with the Regulation.

18. The Rights of Data Subjects

18.1 The Regulation sets out the following rights applicable to Data Subjects:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure (also known as the 'right to be forgotten');
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights with respect to automated decision-making and profiling.

19. Keeping Data Subjects Informed

19.1 The Data Subjects should be aware of the following:

The identity of the Data Protection Officer is Daniel Muscalu who may be contacted via email on daniel.muscalu@ellernemede.org or by telephone on 07470 755084

1. The purpose(s) for which the Personal Data is being collected and will be processed (as detailed in Schedule 1 of this Policy) and the legal basis justifying that collection and processing as stated in Paragraph 5 and 9 of this Policy;
2. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the Personal Data which the Company shall inform the Data Subjects of from time to time;
3. Where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed as stated in Schedule 3 of this Policy;
4. Where the Personal Data is to be transferred to one or more third parties, details of those parties as stated in Schedules 3 and 4 of this Policy;
5. Where the Personal Data is to be transferred to one or more third parties, details of those parties as stated in Schedules 3 and 4 of this Policy;
6. Where the Personal Data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Schedule 4 of this Policy for further details concerning such third country data transfers);
7. Details of the length of time the Personal Data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined) as stated in Schedule 5 of this Policy;
8. The Data Subject may contact the DPO, Daniel Muscalu at any time via email on daniel.muscalu@ellernmede.org] or by telephone on 07470 755084 for the following:
9. To withdraw their consent to the Company's processing of their Personal Data at any time unless there is a legal reason why this may not be possible;
10. For more details on their right complain to the ICO Office (the 'Supervisory Authority' under the Regulation);

11. For further details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it;
12. For details of any automated decision-making that will take place using the Personal Data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.
13. The information set out above in paragraph 19.1 shall be provided to the Data Subject at the following applicable time: Where the Personal Data is obtained from the Data Subject directly, at the time of collection; Where the Personal Data is not obtained from the Data Subject directly (i.e. from another party): If the Personal Data is used to communicate with the Data Subject, at the time of the first communication; or if the Personal Data is to be disclosed to another party, before the Personal Data is disclosed; or in any event, not more than one month after the time at which the Company obtains the Personal Data.

20. Data Subject Access

20.1 A Data Subject may make a Subject Access Request ("SAR") at any time to find out more about the Personal Data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension). The Company is bound by its regulatory bodies and guidance, including but not limited to the CQC and therefore, any SAR will be subject to the CQC and the guidance and rules of any other regulatory body by which the Company is bound. In the event that the Company is legally prevented from disclosing certain information the Company shall inform the Data Subject (or their parent or legal guardian as the case may be) for the reason for non- disclosure.

1. All subject access requests received must be forwarded to the Company's Data Protection Officer.
2. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

21. Rectification of Personal Data

21.1 If a Data Subject informs the Company that Personal Data held by the Company is inaccurate or incomplete, requesting that it be rectified, the Personal Data in question shall be rectified, and the Data Subject informed of that rectification, within one month of receipt the Data Subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

21.2 In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of any rectification of that Personal Data.

22. Erasure of Personal Data

22.1 Data Subjects may request that the Company erases the Personal Data it holds about them in the following circumstances:

1. It is no longer necessary for the Company to hold that Personal Data with respect to the purpose for which it was originally collected or processed;
2. The Data Subject wishes to withdraw their consent to the Company holding and processing their Personal Data;
3. The Data Subject objects to the Company holding and processing their Personal Data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 24 of this Policy for further details concerning Data Subjects' rights to object);
4. The Personal Data has been processed unlawfully;
5. The Personal Data needs to be erased in order for the Company to comply with a particular legal obligation;
6. The Personal Data is being held and processed for the purpose of providing information society services to a child.

However, the Data Subjects right of erasure is subject to the Company's regulatory requirements and consequently the right to erasure of medical records is not an absolute right but subject to restrictions. The GDPR recognizes that the exceptions to the right of erasure includes is limited in relation of medical data and in relation to the provision or management of health or social care. In some cases, records must be kept for a period of 10 years after the death of the patient. Therefore, the right to erasure must be examined on a case by case basis.

22.2 Unless the Company has reasonable grounds to refuse to erase Personal Data as above, all requests for erasure shall be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

22.3 In the event that any Personal Data that is to be erased in response to a Data Subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

23. Restriction of Personal Data Processing

23.1 Data Subjects may request that the Company ceases processing the Personal Data it holds about them. This right is subject to the Company's regulatory requirements and consequently the right to erasure of medical records is not an absolute right but subject to restrictions. This is particularly in relation to patients who are receiving a mandatory health service.Where a request is made and the Company is permitted to comply with such requests, the Company shall retain only the amount of Personal Data pertaining to that Data Subject that is necessary to ensure that no further processing of their Personal Data takes place and that it is archived in an anonymized/ psuedonymised form.

23.2 In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so)

24. Automated Decision Making

24.1 The Company may process Personal Data using automated means. An automated decision is a decision which is made following processing of personal data solely by automatic means, where no humans are involved in the decision-making process ('Automated Decision Making'). If Automated Decision-Making is to be adopted as a process by the Company, the Company shall first ensure that it obtains explicit written consent from the Data Subject in accordance with paragraph 7 of this Policy.

24.2 Where the Company uses Personal Data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on Data Subjects, Data Subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

24.3 The right described in Part 23.1 does not apply in the following circumstances:

1. The decision is necessary for the entry into, or performance of, a contract between the Company and the Data Subject;
2. The decision is authorised by law; or
3. The Data Subject has given their explicit consent.

24.4 Data Subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

24.5 Where Data Subjects have given their consent to the Company to process their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the Data Subject, Data Subjects have the legal right under the Regulation to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other data Controllers, e.g. other organisations).

24.6 Where technically feasible, if requested by a Data Subject, Personal Data shall be sent directly to another Data Controller, including but not limited to, the patient's General Practitioner (GP), dietician, psychiatrist and parents/ legal guardian.

24.7 Where the Company is permitted to comply with a request from a Data Subject (or their parent or legal guardian as the case may be),the Company shall comply with the requests for copies of Personal Data within one month of the Data Subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

24.8 Where data subjects have given their consent to the Company to process their Personal Data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the Data Subject or where such processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services Data Subjects have the right, under the GDPR, to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other Data Controllers).

24.9 Where technically feasible, if requested by a Data Subject, Personal Sata shall be sent directly to the required Data Controller.

24.10 All requests for copies of Personal Data shall be complied with within one month of the Data Subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the Data Subject shall be informed.

25. Objections to Personal Data Processing

25.1 Data Subjects may have the right to object to the Company processing their Personal Data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or medical purposes unless there is a legal reason which requires the Company to refuse such requests. The request will need to be determined on a case by case basis and may differ between patients who have been admitted voluntarily and those who are receiving mandatory treatment.

25.2 Where a Data Subject objects to the Company processing their Personal Data based on its legitimate interests and the Company is legally permitted to give effect to such request, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms, the processing is necessary for the conduct of legal claims or that such processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services.

25.3 Where a Data Subject objects to the Company processing their Personal Data for direct marketing purposes, the Company shall, where legally permitted, cease such processing forthwith.

25.4 Where a Data Subject objects to the Company processing their Personal Data for scientific and/or historical research and statistics purposes, the Data

Subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest or where processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services.

26. Profiling

26.1 Where the Company uses Personal Data for profiling purposes, the following shall apply:

1. Clear information explaining the profiling will be provided, including its significance and the likely consequences;
2. Appropriate mathematical or statistical procedures will be used;
3. Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
4. All Personal Data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 21 and 22 of this Policy for more details on data security).

The Company may use the non- identifiable data of the Data Subject for research purposes. The processing shall, therefore, be in accordance with Article 89 such that the processing is 'necessary for scientific research in accordance with safeguards'. In accordance with the above, the Company shall ensure that appropriate technical and organizational measures are in place including fully anonymizing (pseudonymising) the data to ensure that the data cannot be attributed to any particular patient.

27. Personal Data

27.1 The Personal Data that may be collected, held, and processed by the Company is outlined under Schedule 1 to this Policy. A full list of the exact data may be available on request pursuant to Paragraph 20 of this Policy

27.2 Schedule 1 will be regularly updated by the Company from time to time and shall be regularly reviewed by the Company's DPO.

28. Data Protection Measures

28.1 The Company collects, processes and transfers Personal Data in both electronic copy form and hard copy form in accordance with this Policy.

28.2 The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with Personal Data:

1. emails containing Personal Data must be encrypted via strong passwords;
2. emails containing Personal Data must contain a confidential information discloser at the end of the email which states that if the email has been sent in error the recipient must immediately cease reading the email or downloading any attachments and must not disclose its contents. In addition, the email and any attachments must be deleted irretrievably;
3. where any Personal Data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be secretly deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely including any daily, weekly and monthly backups of data;
4. Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
5. Personal Data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
6. Personal Data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files (downloads) associated therewith should also be deleted;
7. where Personal Data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
8. where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a) Royal Mail Tracked Delivery; b) Parcel Force tracked services; or c) Personal courier;
9. where Personal Data is to be transferred in an electronic copy form it should be passed directly in a password protected and encrypted PDF

document to the Company;

10. no Personal Data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any Personal Data that they do not already have access to, such access should be formally requested from the Data Protection Officer, Daniel Muscalu;
11. all hardcopies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
12. No Personal Data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Protection Officer, Daniel Muscalu;
13. Personal Data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
14. If Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
15. No Personal Data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer, Daniel Muscalu and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
16. No Personal Data should be transferred to any device personally belonging to an employee and Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
17. All Personal Data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted using one- way encryption;
18. All electronic copies of Personal Data should be stored securely using

passwords and data encryption;

19. All passwords used to protect Personal Data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;
20. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff and contractors do not have access to passwords;

28.3 The Company shall obtain the prior express Consent of the Data Subject before sending out any marketing material at the time of first engagement with the Data Subject. Such Consent shall be obtained via the Company's online form which is based on the Company's website. The Data Subject may change their marketing preferences or opt out at any time. Where a Data Subject has opted out, the Company shall remove their details from any marketing database without undue delay.

Where the Data Subject has contacted the Company in relation to an enquiry but has not opted in to receive marketing materials the Data Subject shall still receive the Company's general communication. The Data Subject's data provided to the Company for general communication purposes shall be stored securely on the Company's Customer Relationship Management Systems (CRM Systems). The Company shall comply with the technical and organisational measures as set out in this Policy and its retention period as set out in Schedule 5 of this Policy in respect of such data.

Where Personal Data held by the Company is used for marketing purposes, the Company's marketing officer from time to time (the 'Marketing Officer') has the responsibility of ensuring that the marketing preferences of the Data Subject is correct, that any consents have been obtained before sending out any marketing material and to ensure that any Data Subjects who have opted out of receiving marketing materials do not receive any such material, including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Services. The Marketing Officer shall report to the Data Protection Officer.
A copy of such consent will be retained by the Company within the CRM in accordance with this policy.

1. For the purposes of Direct Marketing, we may retain the email addresses

of data subjects who we have had business with, unless they have opted out.

2. We will clearly record any telephone marketing calls made by us. We will note when the call was made, the duration of the call and what was discussed, using the CRM.
3. Additionally, we will keep track of whether the person contacted was agreeable to being contacted again during the six monthly check on opt-out status.

28.4 Where a multiple-recipient marketing e-mail is sent out by the Company, the Company shall ensure all recipients are blind carbon copied (Bcc) into the email so that the other recipients are unable to identify or receive Personal Data of the other recipients.

28.5 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

28.6 No software may be installed on any Company-owned computer or device without the prior approval of the Data Protection Officer, Daniel Muscalu.

29. Organisational Measures

29.1 The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, Personal Data in order to carry out their assigned duties correctly shall have access to Personal Data held by the Company;
3. All employees, agents, contractors, or other parties working on behalf of the Company handling Personal Data will be appropriately trained to do so;
4. All employees, agents, contractors, or other parties working on behalf of

the Company handling Personal Data will be appropriately supervised;

5. Methods of collecting, holding and processing Personal Data shall be regularly evaluated and reviewed;
6. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling Personal Data shall be regularly evaluated and reviewed;
7. All employees, agents, contractors, or other parties working on behalf of the Company handling Personal Data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
8. All agents, contractors, other parties working on behalf of the Company handling Personal Data must ensure that any and all of their employees who are involved in the processing of Personal Data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation; and
9. Where any agent, contractor or other party working on behalf of the Company handling Personal Data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

30. Transferring Data to a Country Outside the EEA

30.1 The Company may from time to time transfer ('transfer' includes making available remotely) Personal Data to countries outside of the EEA. Any transfers made outside the EEA are as set out in Schedule 3 to this Policy. The Company shall ensure that Schedule 3 is regularly reviewed and updated where necessary.

30.2

1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for Personal Data;
2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
3. The transfer is made with the informed consent of the relevant Data Subject(s);
4. The transfer is necessary for the performance of a contract between the Data Subject and the Company (or for pre-contractual steps taken at the request of the Data Subject);
5. The transfer is necessary for important public interest reasons;
6. The transfer is necessary for the conduct of legal claims;
7. The transfer is necessary to protect the vital interests of the Data Subject or other individuals where the Data Subject is physically or legally unable to give their consent; or
8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

31. Data Breach Notification

31.1 All Personal Data breaches must be reported immediately to the Company's Data Protection Officer, including in the event that any data is missing or appears to have been tampered with.

31.2 If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

31.3 In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described under Part 30.2) to the rights and freedoms of Data Subjects, the Data Protection Officer must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

31.4 Data breach notifications shall include the following information:

1. The categories and approximate number of Data Subjects concerned;
2. The categories and approximate number of Personal Data records concerned;
3. The name and contact details of the Company's Data Protection Officer (or other contact point where more information can be obtained);
4. The likely consequences of the breach; and Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

32. Implementation of Policy

32.1 This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

32.2 We reserve our right to change this Policy and any Schedules at any time without notice to you so please check back regularly to obtain the latest copy of this policy.

SCHEDULE 1: Personal Data

Below is an example of the type of Personal Data the Company controls and processes:

Category of Personal Data held	**Purpose for which the data is collected, held and processed**	**Type of Data**	**Lawful basis for processing including basis of legitimate interest**
Personal details: Including but not limited to contact details, names, addresses, telephone numbers, e-mail addresses, date of birth, place of birth, race/ ethnic origin and nationality.	To identify the Data Subject	Personal Data and Sensitive Personal Data	Necessary for the performance of the contract.
Family and lifestyle details: Including but not limited to the contact details, names, addresses, telephone numbers and e-mail addresses of family members and next of kin details.	To identify the impact that this may have on the Data Subject's health.	Personal Data and Sensitive Personal Data	Necessary for the performance of the contract.
Medical data including Biometric Data, Genetic Data and Data Concerning Health	To provide the relevant level of care/ services and level of care to the patients	Sensitive Personal Data	Processing is necessary for the purposes of preventative or occupational medicine, for the provision of health or social care or treatment or the management of health or social care systems and services and for the assessment of the working capacity of an employee. It is also required for medical diagnosis, the provision of health and social care, treatment and services on the basis of Union or Member State law or

			pursuant to contract with Company or third party health professionals.
Contractual Details: Including but not limited to the contract and details in relation to the contract with the Client, (Patient, Parent, Funder) the Company's Employees, and with the Data Subject.	In order to provide the relevant services to the data subject.	Personal Data	Processing is necessary for the performance of the contract.
Financial Details: Including but not limited to bank account details (sort code, account number), relevant tax codes, national insurance numbers.	To pay employee salaries, to invoice patients, and to fulfil any other payments on behalf of the company	Personal Data	Processing is necessary for the performance of the contract Explicit consent of the Data Subject has been obtained Processing is necessary for a legitimate business interest

The actual full details of any Personal Data held by the Data Subject is contained separately to this Policy and shall be updated from time to time. The full details of the Personal Data held will be held as relevant, either in CareNotes, in a CRM or in an excel spreadsheet, all of which form part of the Company's secure Computer Systems, on site servers, off site back up and redundancy-proof systems. In process of transfer or transmission the personal data shall be pseudonymised, password protected and encrypted.

Schedule 1 will be regularly updated by the Company from time to time and shall be regularly reviewed by the DPO.

SCHEDULE 2: The Company and Third Party Controllers

Oak Tree Forest Limited t/a Ellern Mede, a company incorporated in England and Wales registered number registered 07071928 whose registered office is at 523 Highgate Studios, 53-79 Highgate Road, London, NW5 1TL.

The Hospital provides eating disorder treatment patients. The School aims to provide an education service which is relevant, complementary to and consistent with the eating disorder treatment programmes at Ellern Mede Ridgeway, Ellern Mede Barnet or other service providers.

The Data Protection Officer is Daniel Muscalu who may be contacted via email on daniel.muscalu@ellernmede.org or by telephone on 07470 755084.

Third Party Controllers

The Company may transfer or collect data from Third Party Controller and Processors including pathologists, the Data Subjects general practitioner, healthcare providers and family members/ next of kin. The data is collected and transferred in order for the Company to provide the appropriate level of care and the relevant services to the Data Subject.

As part of the Company's patients continued treatment, the Company may be required to transfer the reports and letters regarding the patients care to their registered general practitioner ('GP'), next of kin, psychiatrist, dietician and/or any consultant or medical practitioner that may be required to have access to the reports or letters in order to act in the patient's best interests. This type of transfer is authorised under the lawful basis that it is necessary for '*preventive or occupational medicine… medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'.*

The Company shall ensure that when it transfers data or receives data from a Third Party Controller it shall carry out an appropriate level of due diligence to ensure that the Third Party complies with its GDPR obligations which may include asking the Third Party in writing how they are complying with GDPR obligations (where appropriate) and/ or ensuring the Company's contract with the Third Party Controller outlines the Third Party Controller's obligations under the GDPR in relation to the transferred Personal Data. The Company shall not accept data from Third Party Controllers which does not comply with the GDPR.

This Schedule 2 will be regularly updated by the Company from time to time and shall be regularly reviewed by the DPO.

SCHEDULE 3: Data Processing in EEA

Patient data may be transferred outside the EEA where the patient comes to Ellern Mede from a country outside the EEA. In order to provide the relevant services and treatment for the patient, it may be necessary to transfer Personal Data to third parties within the non- EEA country that the patient is originally from, including but not limited to, health professionals and parents.

When personal data is to be sent electronically to non- EEA countries it will be pseudonymised, encrypted or password protected to the same standards as within the EEA. Where information requires to be posted, this will be by tracked courier delivery services.

Lawfulness of Processing Personal Data outside the EEA

We shall only transfer Personal Data to public authorities outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

This Schedule 3 will be regularly updated by the Company from time to time and shall be regularly reviewed by the DPO.

SCHEDULE 4: Purpose for which Data is Processed

The Company controls and processes Personal Data in both hard copy and electronic format.

Where consent is required, he Company shall obtain full and explicit consent directly from the Data Subject pursuant to paragraph 7 of the Policy for the control and processing of Personal Data not lawfully required in terms of the delivery of the contract of service.

The Company shall inform the Data Subject of the intention to securely deliver their Personal Data to a third-party as listed in Schedule 2 of this Policy.

Where consent is required, the Company shall also obtain written consent in accordance with paragraph 7 of this Policy before any such Personal Data is transferred for the Purpose.

The Data Subject's Personal Data must be sent to the Company by the referrer or funder in a pseudonymised format. The Company shall not accept, control or process any Personal Data which is not sent in a secure pseudonymised (anonymised) format.

The Company shall ensure that they have seen (either in physical hard copy form or electronic form) written explicit consent obtained by the third party, including not limited to, the funder, referrer, parent and/ or guardian, from the Data Subjects where the data subject is 16 or over, showing that the third party is duly authorised (by receiving this written consent) to process and control the Data Subject's Personal Data.

Technical Data Security Measures

- All emails containing Personal Data must be encrypted;
- All emails containing Personal Data must be marked 'confidential';
- Personal Data may only be transmitted over secure networks;
- Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- Personal Data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- Where Personal Data is to be transferred in hardcopy form, it should be passed directly to the recipient in accordance with this Policy;
- All Personal Data transferred physically should be transferred in a suitable container marked "confidential";

- No Personal Data may be shared informally and if access is required to any Personal Data, such access should be formally requested from the DPO;
- All hardcopies of Personal Data, along with any electronic copies stored on physical media should be stored securely;
- No Personal Data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
- Personal Data must be handled with care at all times and should not be left unattended or on view;
- Computers used to view Personal Data must always be locked before being left unattended;
- No Personal Data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the DPO and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
- No Personal Data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;
- All Personal Data stored electronically should be backed up regularly with backups stored onsite. All backups should be encrypted;
- All electronic copies of Personal Data should be stored securely using passwords and encryption;
- All passwords used to protect Personal Data should be changed regularly and should must be secure;
- Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
- No software may be installed on any Company-owned computer or device without approval; and

- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the DPO to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Organisational Data Security Measures

The following organisational measures are in place within the Company to protect the security of personal data:

- All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy;
- Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
- All employees and other parties working on behalf of the Company handling Personal Data will be appropriately trained to do so;
- All employees and other parties working on behalf of the Company handling Personal Data will be appropriately supervised;
- All employees and other parties working on behalf of the Company handling Personal Data should exercise care and caution when discussing any work relating to Personal Data at all times;
- Methods of collecting, holding, and processing Personal Data shall be regularly evaluated and reviewed;
- The performance of those employees and other parties working on behalf of the Company handling Personal Data shall be regularly evaluated and reviewed;
- All employees and other parties working on behalf of the Company handling Personal Data will be bound by contract to comply with the GDPR and this Policy;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and this Policy;
- Where any agent, contractor or other party working on behalf of the Company handling Personal Data fails in their obligations under the GDPR and/ or this Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.
- In order to ensure the safety of all patients, any visitors to the Company's premises or temporary or agency workers must be clearly identifiable i.e. agency staff wear

wristband fobs which are access controlled daily; preceptorship temporary staff wear green lanyards; full time staff members wear black lanyards. Visitors or Contractors are supervised at all times by our staff.

SCHEDULE 5: Data Retention Policy

Introduction

This schedule sets out the obligations of the Company regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

Aims and Objectives

The primary aim of this Schedule is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Schedule aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Schedule also aims to improve the speed and efficiency of managing data.

Data Disposal

Upon the expiry of the data retention periods set out in the table below of this Schedule, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- Personal data stored in hardcopy form shall be shredded;
- Special category personal data stored in hardcopy form shall be shredded.

Data Retention

- As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
- Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.
- When establishing and/or reviewing retention periods, the following shall be considered:
    - The objectives and requirements of the Company;
    - The type of personal data in question;

- The purpose(s) for which the data in question is collected, held, and processed;
- The Company's legal basis for collecting, holding, and processing that data; and
- The category or categories of data subject to whom the data relates.

- If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
- Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).
- In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria
Patient/ Family Personal Details	Names, addresses, telephone numbers, e-mail addresses.	So that we may contact the patient and enter into a contract with the patient to provide the relevant services.	Annually.	GP Records may be retained until 10 years after the patient's death or after the patient has permanently left the country. In the case of a child if the illness or death could have potential relevance to adult conditions or have genetic implications for the family of the deceased, clinicians may retain the record for a longer period. Records relating to mental disorder within the meaning of mental health legislation can be kept until 20 years after the date of the last contact; or 10 years after the patient's death – whichever is sooner. GP or Hospital records of children and young people (16 years on admission until the patient's 25th birthday or 26th if an entry was made when the young person was 17; or 3 years after death of the patient if sooner.
Patient/ Family Medical Details	Medical data relating to the physical health of the patient.	So that we can provide an accurate diagnosis, treatment and prescriptions to the patient.	Annually.	GP Records may be retained until 10 years after the patient's death or after the patient has permanently left the country. In the case of a child if the illness or death could have potential relevance to adult conditions or have genetic implications for the family of the deceased, clinicians may retain the record for a longer period. Records relating to mental disorder within the meaning of mental health legislation can be kept until 20 years after the date of the last contact; or 10 years after the patient's death – whichever is sooner. GP or Hospital records of children and young people (16 years on admission until the patient's 25th birthday or 26th if an entry was made when the young person was 17; or 3 years after death of the patient if sooner.

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria
Patient Financial Details	Financial details including their account number, sort code, name on card and billing address.	In order to take payment from the Client for the services provided.	Weekly.	The data shall be deleted as soon as payment has been taken.