7. Data Protection Policy

1. Introduction

This Policy sets out the obligations of CNELM, a company registered in England and Wales under number 08635327, whose registered office is at 14 Rectory Road WOKINGHAM, RG40 1DH ("the Company") regarding data protection and the rights of applicants, students, graduates and exited students, clinic and coaching clients related to the Supervised Student Training Clinic, Partners and business contacts, and emergency contacts and individuals that pay on behalf of students in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. 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.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 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.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 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 it is processed, is erased, or rectified without delay.

2.5 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 GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 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.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of

this policy indicated for further details):

3.1 The right to be informed (Part 12).
3.2 The right of access (Part 13);
3.3 The right to rectification (Part 14);
3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);
3.5 The right to restrict processing (Part 16);
3.6 The right to data portability (Part 17);
3.7 The right to object (Part 18); and
3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

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

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;
4.1.2 The 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 with them;
4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;
4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;
4.1.5 The 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 data controller; or
4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data 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.

4.2 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:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the EU or EU Member State law prohibits them from doing so);
4.2.2 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 the 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);
4.2.3 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;
4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aims, 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;
4.2.5 The processing relates to personal data which is clearly made public by the data subject;
4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 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;

4.2.8 The processing is necessary for the purposes of preventive 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;

4.2.9 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

4.1.10 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.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from employee data subjects and

5.1.2 Personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 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 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

9. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 The Company's Data Protection Officer is Dave Lee dave@cnelm.co.uk

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which the Company collects, holds, and processes personal data;

10.3.3 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;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3. Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 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 Part 28 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of personal data and details of any consequences of failing to provide it; and

12.2.12 We do not deploy any automated decision making or profiling.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at dave@cnelm.co.uk

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Company's Data Protection Officer.

13.5 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.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete. Students and Staff have direct access to edit their profile information and basic personal data directly on the CNELM Moodle Platform.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
15.1.3 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 18 of this Policy for further details concerning the right to object);
15.1.4 The personal data has been processed unlawfully;
15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, 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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's 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).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 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).

17. Data Portability

17.1 The Company does not process personal data using automated means.

17.2 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following formats:

17.2.1 PDF, Microsoft Office Document, other machine readable formats such as csv files. Data will be sent using password protected and encrypted archives such as RaR and 7z.

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 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.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.
18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18.4 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 GDPR, "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.

19. Automated Decision-Making

19.1 The Company does not use personal data in automated decision-making processes.

20. Profiling

20.1 The Company uses personal data for profiling purposes in order to comply with expectations for Higher Education relevant professional associations. Where applicable such data may be published in anonymised reports.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
20.2.1 Appropriate mathematical or statistical procedures shall be used;
20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Type of Data	Data Reference	Purpose of Data
Application Form: Personal and Special Category Data	**Reference A** - enquiry, applicant, student, graduate and exited student	Contractual and Legitimate Interests. Vital Interest in respect of emergency contact and med information
Assessment of Prior and Experiential Learning Docs - Personal Data	**Reference A**	Contractual and Legitimate Interests
ID Proof - Personal and Special Category Data	**Reference A**	Contractual and Legitimate Interests, Legal Obligation
Entry Requirement Doc - Personal Data	**Reference A**	Contractual and Legitimate Interests,
CV (optional) - Personal and Special Category Data	**Reference A**	Consent
Invoices - Personal Data	**Reference A**	Contractual
Credit Notes - Personal Data	**Reference A**	Contractual
Receipts - Personal Data	**Reference A**	Contractual
Payment Schedules - Personal Data	**Reference A**	Contractual
Statements of Account - Personal Data	**Reference A**	Contractual
DD forms and Bank Transfer Personal and Special Category Data	**Reference A**	Contractual
Offer Letter - Personal Data	**Reference A**	Contractual
Study Plan - Personal Data	**Reference A**	Contractual
Additional Information - None	**Reference A**	Contractual
Fees and Finance - Personal Data	**Reference A**	Contractual

Confirmation Agreement - Personal Data	**Reference A**	Contractual
Fitness to Study and Practice	**Reference A**	Contractual, Legitimate Interest and Legal
Confirmation of Practice - Personal and Special Category Data	**Reference A**	Contractual, Legitimate Interest and Legal
BANT Practice student guidelines - None	**Reference A**	Contractual
References - Personal and Special Category Data and third party	**Reference A**	Legitimate Interest
Enrolment Letter - yearly - Personal Data	**Reference A**	Contractual and Legitimate Interest
BEC, Degree, NTPD, NCD, DE, CPD Certs and NTPD Statement of Achievement - Personal Data	**Reference A**	Contractual, Legitimate Interest and Legal
Transcripts - Personal Data	**Reference A**	Contractual, Legitimate Interest and Legal
BANT Membership - Personal Data	**Reference A**	Legitimate Interest
Fitness to Practice Declarations - Personal and Special Category Data	**Reference A**	Public Task, Vital Interests, Contractual
Alumni - Personal Data	**Reference A**	Contractual, Consent and Legitimate Interest
Extenuating circumstances - including supporting evidence - Personal and Special Category Data	**Reference A**	Contractual (i.e. MU Regs), Legitimate Interests
Interruption of Studies - including if submitted supporting evidence - Personal and Special Category Data	**Reference A**	Contractual (i.e. MU Regs), Legitimate Interests
Academic Misconduct - Personal and Special Category Data	**Reference A**	Contractual (i.e. MU Regs), Legitimate Interests, Public Task
Complaints and Appeals and Concerns - Personal and Special Category Data	**Reference A**	Contractual (MU Regs, NTEC Requirements), Legitimate Interests, Public Task
Non-disclosure Agreements - Personal and Special Category Data	**Reference A**	Contractual and Legal
Bursary - Personal and Special Category Data	**Reference A**	Contractual and Legitimate Interests
Learning Needs Assessments - including supporting evidence - Personal and Special Category Data	**Reference A**	Contractual and Legal and Legitimate interests
AEAR 1 or 2 Applications - Personal and Special Category Data	**Reference A**	Contractual and Legitimate interests
Pastoral and Coach Mentor Support - Personal and Special Category Data	**Reference A**	Consent, Legitimate and Vital Interests, Legal Obligation and Public Task
See Employee Data Protection Policy	**Reference B - Staff (PAYE and Flexible Fee Contract)**	

Client Enquiry Documents - Personal and Special Category Data	**Reference C**	Consent, Legitimate and Vital Interest, Legal Obligation, contractual and Public Task
Client Health Records (supplied by client and via the Clinic Supervisor) - Personal and Special Category Data	**Reference C**	Consent, Legitimate and Vital Interest, Legal Obligation, contractual and Public Task
Client Terms of Agreement Personal Data	**Reference C**	Consent and Contractual
Client case recordings - Personal and Special Category Data	**Reference C**	Consent, Legitimate Interest, ,contractual and Public Task
Client complaints, claims and legal action - Personal and Special Category Data	**Reference C**	Consent, Legitimate and Vital Interest, Legal Obligation, contractual and Public Task
Application form, Terms of Agreement, Payment details - Personal Data	**Reference D - Business, Education & Ethics including Research Ethics Committee**	Consent, Legitimate and Vital Interests and Public Task
Application form, right to work in UK - Personal and Special Category Data	**Reference D - External Examiners**	Consent and Contractual
Application form, right to work in UK, payment details - Personal and Special Category Data	**Reference D - External Verifiers**	Consent and Contractual
Application form, Terms of Agreement, right to work in UK, payment details - Personal and Special Category Data	**Reference D - Contributing Lecturers**	Consent, Contractual and Public Task
Name, email contact and address - Personal Data	**Reference D - Exam Invigilators**	Consent, legitimate interests and contractual
Application form, Terms of Hire - Personal and Special Category Data	**Reference D - Venue Hirers**	Consent, legitimate interests, contractual and public task
Memorandum of Cooperation/s and Partnership Agreement, and named contacts including University Link Tutor and Academic Partnerships, payment details	**Reference E - Middlesex University**	Contractual, legitimate and vital interests, legal obligation and public task
Named contacts and contact details, payment details	**Reference E - Nutritional Therapy Education Commission**	Contractual, legitimate and vital interests, legal obligation and public task
Named contacts and contact details, payment details	**Reference E - UK CPD**	Contractual, legitimate and vital interests, legal obligation and public task
Named contacts and contact details, payment details	**Reference E - Federation of Holistic Therapists**	Contractual, legitimate and vital interests, legal obligation and public task
Contact name, email, address and payment details; Personal Data For a list of Third Parties please contact the Data Manager or Managing Director	**Reference F - Other Business contacts:** The Company maintains a contact list of other Business or Governmental third-party service providers engaged in the delivery of services and learning resources.	Contractual, Legitimate Interest and is some cases Legal Obligation and Vital Interests
Named contacts and contact details, payment details	**Reference E - Nutritional Therapy Education Commission**	Contractual, legitimate and vital interests, legal obligation and public task
Minutes of meeting will contain Personal	**Reference G - Meetings: Internal and**	Contractual, Legitimate Interests and in

Data - such as names, Personal identifiers such as student numbers and for some meetings Sensitive Data related to progression issues that could include health details or privileged information	**External Discursive Meetings and Minutes thereof:** The Company in its capacity as a Higher Education Provider will hold meetings, which are recorded and minuted, that include External participants such as Academic Boards related to Degree Programmes, Verification Panels related to the NTPD and NCD Awards, a Business & Education Ethics Committee, a Research Ethics Committee. Various Internal staff meetings also take place that are recorded and minutes taken - these include the Senior Management Team meeting, the Senior Academic Team Meeting, Internal Progression Meetings, other academic meetings for Module and Programme staff. Student Reps are invited to various External and Internal meetings and external participants may be invited to some internal meetings. All meetings are confidential and some participants may only attend relevant parts of some meetings. We ask participants not to print copies of Agendas or Minutes. Some hard copies will be available for those attending in person and must be left in the meeting room and then assigned for shredding by the Centre Administratoror other delegated members of staff. Most meetings will also have a Zoom link option for those attending online. A recording of the Zoom session and a back-up audio recording is made. The audio and/or video files created are then securely stored on the Company's Cloud services (Google Drive) - and where applicable given further protection by the use of 7zip as a password protected archive. We may use a Transcription service, for which we have an account that is compliant with GDPR to upload audio recordings for the purpose of making a transcript and to aid the production of minutes. In the event that we use such a service then the audio recording and transcript will be deleted from the Transcription Service provider's servers as soon as the exported transcript has been created and stored on The Company's Cloud. As soon as the minutes are produced and approved then recordings and transcripts are deleted from The Company's Cloud.	some cases Legal Obligation and Vital Interests Notes on meetings and **Transcription**: Students sign a Confirmation Agreement giving The Company a lawful Contractual Purpose to processing Personal Data insofar as such Data may be captured by recording technologies when attending meetings or contained within the minutes of such meetings if either discussed in a way that the minutes could identify a Person or Person was due to attend and instead sent apologies. Staff have a contractual obligation to attend and part-take in meetings as required by their Contracts, Terms as set out in the Staff Handbook or as a result of their role/job description. Other participants to meetings **who are not staff or students** will be made aware that meetings are recorded and transcription services may be used. Consent from such participants will be gained at the commencement of meetings by the Chair in relation to the use of Transcription Services - if any participant objects they will be invited to either leave the meeting or remain on the understanding that transcription services will not be used. If any participants **who are not staff or student** objects to recordings then they will be invited to leave. A space is provided in most internal meetings for a 'safe space' under Chatham House rules.

22. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

22.1 All emails containing personal data must be encrypted using Gmail HTTPS, secure

email for any Sensitive Data and Rar and 7zip archives as applicable;

22.2 All emails containing personal data, other than name and company email address, must be marked “confidential”;

22.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

22.1 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

22.2 Personal data that is Sensitive contained in the body of an email, whether sent or received, should be deleted and the sender sent a secure email reply with instructions on how to send their data securely. Where compliance to send data more securely is not possible then the data will be copied from the body of that email and stored securely. The email itself will then be deleted. In all circumstances temporary files associated therewith should also be deleted using Google's deletion method and secure erase (Eraser on Windows and Shredder on Mac or Bleachbit on Linux);

22.3 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;

22.4 Where personal data is to be transferred in hard-copy form it should be passed directly to the recipient or sent using Royal Mail or Parcel Force, and

22.5 All personal data to be transferred physically, whether in hard-copy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

23. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to personal data storage.

23.1 All electronic copies of personal data should be stored securely using passwords and 256 data encryption;

23.2 All hard-copies 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;

23.3 All personal data stored electronically should be backed up daily with backups stored onsite **OR** offsite. All backups should be encrypted using industry standard encryption technologies;

23.4 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 dave@cnelm.co.uk or the Head of Quality Assurance kate@cnelm.co.uk 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; and

23.5 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 GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

24. Data Security - Disposal

When 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 securely deleted and disposed of.

For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

25. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

25.1 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 (DPO) dave@cnelm.co.uk;

25.2 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 DPO;

25.3 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;

25.4 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; and

25.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Controller 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.

26. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

26.1 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 can contain a combination of uppercase and lowercase letters, numbers, and symbols. Preferably passwords should use lengthy phrases memorable to the individual e.g. apple.&.pears.fall.down.stairs.apple.pears.

26.2 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 do not have access to passwords;

26.3 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; and

26.4 No software may be installed on any Company-owned computer or device without the prior approval of the Director of IT or Head of Quality Assurance.

27. Organisational Measures

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

27.1 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 GDPR and under this Policy, and shall be provided with a copy of this Policy;

27.2 Only employees, agents, subcontractors, 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;

27.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

27.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

27.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

27.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

27.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

27.8 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;

27.9 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 GDPR and this Policy by contract;

27.10 All agents, contractors, or 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 GDPR; and

27.11 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.

28. Transferring Personal Data to a Country outside the EEA

28.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

28.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

28.2.1 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;

28.2.2 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 the supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); 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;

28.2.3 The transfer is made with the informed consent of the relevant data subject(s);

28.2.4 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);

28.2.5 The transfer is necessary for important public interest reasons;

28.2.6 The transfer is necessary for the conduct of legal claims;

28.2.7 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

28.2.8 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.

29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

29.2 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.

29.3 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 29.2) 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.

29.4 Data breach notifications shall include the following information:

29.4.1 The categories and approximate number of data subjects concerned;

29.4.2 The categories and approximate number of personal data records concerned;

29.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
29.4.4 The likely consequences of the breach;
29.4.5 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.

30. Implementation of Policy

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

This Policy has been approved and authorised by:

Name:	Kate Neil
Position:	Managing Director
Date:	30.11.2020
Due for Review By:	31.01.2021 - subject to change in Legal Requirements

Signature

Named Contact Person/s responsible for this Policy
Kate Neil Managing Director and Head of Quality Assurance kate@cnelm.co.uk
Dave Lee Centre Administrator, Data Manager and Practice Supervisor dave@cnelm.co.uk

8. Data Retention Policy

1. Introduction

This Policy sets out the obligations of CNELM, a company registered in England and Wales under number 08635327, whose registered office is at 14 Rectory Road, WOKINGHAM, RG40 1DH ("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").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a ("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.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, 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.

Under the GDPR, personal data shall be 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. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects

have the right to have their personal data erased (and to prevent the processing of personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
b) When the data subject withdraws their consent;
c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
e) When the personal data has to be erased to comply with a legal obligation; or
f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company and the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. Please see table on page 6 for details of legal purpose and retention.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy 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 Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 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 Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company and by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

a. The Company's servers, located in the UK and Germany
b. Third-party servers, operated by 1 and 1, Google, Microsoft Azure, Telenova, Online 50 and located in the EU. Google and Microsoft also operate within the EU/US Privacy Shield.
c. Computers permanently located in the Company's premises at 14 Rectory Road, WOKINGHAM, RG40 1DH.
d. Laptop computers and other mobile devices provided by the Company to its employees, where permitted and with restrictions as outlined in the Data Protection Policy
e. Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Employee Data Protection Policy and where relevant within the terms of Data Processing Agreements.
f. Physical records are stored in locked drawers or filing cabinets, either at the Company's premises or other approved employees premises. Physical records taken away from an approved premises are stored in a locked password protected case or file.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined,

the criteria by which the retention of the data will be determined).

4.2.. Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling, as set out in the Company's Data Protection Policy.

5. Technical and Organisational Data Security Measures

1.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;
b) All emails containing personal data must be marked "confidential";
c) Personal data may only be transmitted over secure networks;
d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
e) 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;
f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
g) Where sensitive personal data is to be transferred in hard-copy form, it should be passed directly to the recipient or sent by Royal Mail or Parcel Force delivery services, and signed for as appropriate.
h) All personal data transferred physically should be transferred in a suitable container marked "confidential";
i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Data Manager.
j) All hard-copies of personal data, along with any electronic copies stored on physical media should be stored securely;
k) 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;
l) Personal data must be handled with care at all times and should not be left unattended or on view;
m) Computers used to view personal data must always be locked before being left unattended;
n) 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 Data Protection Officer 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;
o) 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;
p) All personal data stored electronically should be backed up offsite**.** All backups should be encrypted;
q) All electronic copies of personal data should be stored securely using passwords and encryption;
r) All passwords used to protect personal data should be changed regularly and must be secure;
s) 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;
t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

u) No software may be installed on any Company-owned computer or device without approval; and
v) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Manager 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.

1.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) 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 the Company's Data Protection Policy;
b) 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;
c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
e) 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;
f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
h) 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 the Company's Data Protection Policy;
i) 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 the Company's Data Protection Policy;
j) 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 the Company's Data Protection 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.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, orotherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted as appropriate to the device - for example secure deletion software used on local storage devices and industry standard erasure by third party providers such as Google and Microsoft.

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted as appropriate to the device - for example secure deletion software used on local storage devices and industry standard erasure by third party providers such as Google and Microsoft.

6.3 Personal data stored in hard-copy form shall be shredded to at least Level 2 Standard;

6.4 Special category personal data stored in hard-copy form shall be shredded to Level 3 and recycled by a Certificate Shredding Company contracted for this purpose. We use Stream

Shredding (Phoenix Recycling) to undertake this task. Hard-copy Data is placed in a secured/locked box and collected monthly or as required.

7. Data Retention

7.1 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.

7.2 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.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;
b) The type of personal data in question;
c) The purpose(s) for which the data in question is collected, held, and processed;
d) The Company's legal basis for collecting, holding, and processing that data;
e) The category or categories of data subject to whom the data relates;

7.4 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.

7.5 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).

7.6 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.

Date Ref	**Type of Data**	**Purpose of Data**	**Review Period**	**Retention Period or Criteria**	**Comments**
A - Enquiry Courses Employment Clinic	Hardcopy and/or Electronic. Can include personal data.	Respond to and process an enquiry on the basis of legitimate interests and consent that may lead to employment.	3 years	Enquires that do not progress: **Courses** - twenty-four months **Employment** - six months **Clinic** - six months	
A - Application Courses Employment Clinic	Hardcopy and/or Electronic. Will include personal and sensitive data	**Courses** - to process an application and confirm entry requirements leading to a course offer. For contractual, vital and legitimate interests and legal purposes. **Employment** - application and interview purposes in order to select candidates for the job offer. For contractual, vital	3 years	**Courses** - twenty-four months if application does not progress **Employment** - for six months if application does not progress and applicant does not consent in writing for us to retain details for future opportunities.	For purposes of annual monitoring.

		and legitimate interests and legal obligations. **Clinic** - appraise suitability for participation in Supervised Student Training Clinic. For contractual, vital and legitimate interests and legal obligations.		**Clinic** - if applicant does not proceed to a consultation then data deleted within six months.	
B - Students	Electronic with occasional hardcopy and includes both personal and sensitive data. Data processed for contractual, legal obligation, legitimate and vital interest purposes and on some occasions for public tasks.	Deliver course content, to: - facilitate payment of course fees by self or third party - collection of emergency contact person/s details for safeguarding purposes - enable access to course materials - enable submission of assessments, and access to marking and feedback - Support student enrolment, progression and engagement - pastoral and coach mentor support - ensure inclusivity - respond and process student deferment requests - respond and process student complaints and appeals - present student data for ratification of assessments and conferment of awards - collecting student feedback - undertake first destination statistics and graduate surveys	5 years for programme subject review	Two years following dispatch of final award for course undertaken, or if a student withdraws from study for any reason.	1 - some data will be kept indefinitely related to transcripts and awards. 2 - finance data kept in compliance with HMRC requirements; and in exceptional cases for legal pursuit of debt. 3 - data may be retained longer for purposes of revalidation and renewal of accreditation of course, or for legal purposes. 4. Documentation related to pastoral and coach mentor support will be retained in accordance with the Statute of Limitations.
B - Staff	Electronic with occasional hardcopy and includes both personal and sensitive data.	Enable: - Induction - Staff Support and Development - Performance Review	5 years	Six years in respect of Statute of Limitations at the point at which leaves our employment for	1 - data can be retained longer if required by law. 2 - data in relation to pensions will be retained

	Data processed for contractual, legal obligation, legitimate and vital interest purposes and on some occasions for public tasks.	- Payment and processing for - PAYE and contract services - Provision of a Contract of Employment - Access to resources to fulfill job role - quality management		any reason.	indefinitely.
B - Clinic	Electronic with occasional hardcopy and includes both personal and sensitive data. Data processed for, consent, contractual, legal obligation, and legitimate and vital interest purposes and on some occasions for public tasks.	- provide clients with a nutritional therapy or dietary educator consultation or a coaching consultation. - provide students with a learning opportunity to work with clients under supervision for nutritional therapy and dietary educator consultations and under guidance for coaching consultations. - enable students to submit clinic and coaching anonymised assessments and receive feedback - enable clients to provide feedback - enable clients to consent to further participation in clinic services.	3 years	As anonymised client data is linked with students then retention of client data is likewise linked to retention period for students. This will be a minimum of two years following students' graduation or withdrawal from studies - unless there is a legal reason to keep Data for longer or if a Client sees another practitioner. After a consultation clients are asked to provide feedback, including sur	Data may be retained for longer if required by law. The Clinic Supervisor will retain client data for nutritional therapy and dietary educator consultations in accordance with the law and regulating body. Coaching client data will be held by Client's insured Practitioner Coach in accordance with regulatory requirements
C - Graduates	Electronic data for legitimate, contractual, consent and public task purposes	The consent purpose relates to graduates who opt to join our graduate group, alumni services or to continue to receive information related to continuing professional development (CPD) opportunities. Contractual and public task purposes relate to higher education expectations for collecting graduate data	5 years	As above for B - Students, when a graduate leaves an alumni programme or withdraws consent for continuing contact.	C - Graduates

		Legitimate interests in promoting CPD and Job Opportunities			
C - Prior Employees	Personal and Sensitive Data	For Pensions, Company and audit regulations and requirements	As required by Law	To fulfil ongoing obligations - including provision of references, pensions etc.	Indefinitely for the continuing fulfilment of Contractual and Legal Obligations
Other Stakeholders - including Contractors, Suppliers and Service Providers. This will also include Contact Details of Data Subjects who hire our venue.	Personal Data and where applicable for Legal Obligations Sensitive Data (such as evidence of 'right to work in UK')	Contractual and Legal Obligation: To fulfil contractual requirements and to deliver services	2 years after end of contract or service or longer if required by Law	As a provider of Higher Educational Services and as a Business we maintain records of names and contact details of a range of contractors, suppliers and service providers. These include providers of Learning resources, alternate exam invigilation service providers, External Examiners, Contacts with validation and accreditation partners, External Examiners and Verifiers, Contributing Lecturers, Partners, Members of our Ethics Committees etc.	Company details of Stakeholders details may be retained longer if records of activity related to discursive meetings, especially academic boards.
All - Minutes of External and Internal Meeting approved minutes	Personal and sometimes Sensitive Data	To provide an official record of discussion, decisions and agreed Actions for the purpose of tracking, providing evidence of decisions and compliance with Contractual Requirements related to validation of Programmes, compliance with Memorandum of Understanding with validating university.	6 years or longer if required by Law	Retained longer if required by Law. Academic Board minutes retained indefinitely	In addition - accreditation of professional courses and Legal Requirement expected of an Alternative Higher Education Provider.

8. **Roles and Responsibilities**

8.1 The Company's Data Protection Officer is Dave Lee dave@cnelm.co.uk.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

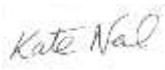
8.3 The Data Protection Officer in conjunction with the Senior Management Team shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company**.**

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. **Roles and Responsibilities**

This Policy shall be deemed effective as of 25/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.
This Policy has been approved and authorised by:

Name:	Kate Neil
Position:	Managing Director
Date:	30.11.2020
Due for Review By:	31.01.2021 - earlier if there is change in Governing Law



Signature

Named Contact Person/s responsible for this Policy
Kate Neil Managing Director and Head of Quality Assurance kate@cnelm.co.uk
Dave Lee Centre Administrator, Data Manager and Practice Supervisor dave@cnelm.co.uk