Contactyoga4health@gmail.com **Tel 07782 413 146**

Charity Number: 1190806

Data Protection Policy

1. Policy Statement

YIHA collect and process personal data about people with whom it deals with in order to carry out its business and provide its services. Such people include but are not limited to (present, past, and prospective) students, members, contractors, volunteers, employees suppliers and other business contacts.

The data may include identifiers such as name, address, email address, data of birth. It may also include private and confidential information, and special categories of personal data. YIHA may also be required to collect and use certain types of such personal information to comply with the requirements of the law.

The lawful and proper treatment of personal information by YIHA is extremely important to the success of our business and in order to maintain the confidence of our service users, stakeholders, and employees. As No matter how it is collected, recorded, (e.g., on a computer or other digital format, hardcopy, paper, or images, including fil) and/or used, personal information will be dealt with properly and compliantly with data protection legislation.

The UK General Data Protection Regulations (GDPR) is a legal framework that initially set out guidelines for the collection and processing of personal data from individuals who live in the European Union (EU). The Brexit transition period ended on 31 December 2020 but the GDPR has been retained as the UK GDPR, and continues to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law.

For the purpose of the Data Protection Act 1998 (the "Act") and General Data Protection Regulation 2018 (GDPR), YIHA is the data controller and the Data Protection Officer is YIHA Institute Manager.

2. Scope

All YIHA staff, volunteers, tutors, students and anyone working for or representing the YIHA, without exception, are within the scope of this policy. Further guidance on data protection for volunteers and students is available in YIHA Data Protection Guidance.

This policy applies to the data protection legislation and principles applicable to processing data from adult data subjects as YIHA does not provide training for those working with children and adolescents. If you are providing yoga classes for children and adolescents outside of your role with YIHA you should be advised that different data protection principles apply to this population.

Further guidance on data protection for children's information is available here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/

3. Introduction to Data Protection

Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it is about building trust between people and organisations. Data protection concerns treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society. The UK data protection regime is set out in the Data Protection Act (DPA) 2018, alongside the UK GDPR (outlined below).

4. The UK General Data Protection Regulatory (GDPR) Principles

The UK GDPR sets out seven key principles that are central to processing personal data. They are set out right at the start of the legislation, and inform everything that follows. Compliance with these key principles is a fundamental building block for good data protection practice and is key to YIHA compliance with the detailed provisions of the UK GDPR. The seven key principles are:

Lawfulness, fairness and transparency: data should be processed lawfully, fairly and in a transparent manner in relation to individuals (see 6.2 below)

Purpose limitation: data should be 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

Data minimisation: data gathering should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed

Accuracy: data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Storage limitation: data should 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 are 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 individuals

Integrity and confidentiality: data should be 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

Accountability: those collecting data must be responsible for, and be able to demonstrate, compliance with the GDPR principles and be accountable for compliant processes as stipulated by UK GDPR and the Data Protection Act 2018. This includes having appropriate measures and records in place to be able to demonstrate this compliance.

5. UK GDPR Terminology

5.1 Personal Data

'Personal data' means information about a particular 'identified' or 'identifiable' living individual (see 5.3 below). This might be anyone, including a customer, service users, employee, student, business contact, public official, member of the public or any other individual you are collecting data about.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information is 'personal data'.

The UK GDPR applies to the processing of personal data that is:

- wholly or partly by automated means e.g. information gathered through online registration forms and websites
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system e.g. paper documents containing personal information such as enrolment forms, pre-exercise readiness health questionnaires and service users intake forms

Personal Data:

- Doesn't need to be 'private' information, even information which is public knowledge or is about someone's professional life can be 'personal data'.
- Doesn't cover truly anonymous information but if you could still identify someone from the details, or by combining it with other information, it will still count as 'personal data'.
- Includes paper records, even if you plan to put them on a computer (or other digital device), and digital records that you collect, such as maintaining service users/ student records for yoga sessions/assessment
- Can include special categories of personal data (see GDPR article 9 and 4.2 below) which must be processed in much more limited circumstances. Special category data is considered sensitive and specifically includes genetic and biometric data where processed to uniquely identify an individual.

5.2 Special Category Data

The GDPR refers to the processing of data that is more sensitive in nature as "special categories of personal data". This means personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply as explained above.

In order to lawfully process special category data, YIHA must identify both a lawful basis (see Section 6 and GDPR Article 6) and a separate condition for processing special category data (GDPR Article 9 also listed in Appendix 1).

A lawful condition for processing special category data includes "the data subject has given explicit consent to the processing of those personal data for one of more specified purposes" and we believe this condition is the most applicable to YIHA practices (see Section 6).

5.3 How is a person identified or identifiable by their personal data?

An individual is **'identified'** or **'identifiable'** if you can distinguish them from other individuals through the personal data that is being gathered/ processed. A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context and a combination of identifiers may be needed to identify an individual. The UK GDPR provides a non-exhaustive list of identifiers, including:

- name;
- identification number;
- location data; and
- an online identifier, including IP addresses and cookie identifiers which may be personal data.

Further information is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#1

5.4 What does 'processing' data mean?

"Processing" is a very broad term relating to a wide range of operations performed on personal data, including by manual or automated means. It includes the 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 of personal data.

Examples of processing data include:

- staff management and payroll administration;
- student enrolment and registration systems;
- service users intake forms and records of yoga sessions;
- access to a contacts database containing personal data;
- shredding/ destroying documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (including CCTV).

6. Lawful Basis to Process Data

Organisations and individuals must have a valid lawful basis in order to process personal data. YIHA believe that item 'clear consent' from the service users/ student (as listed below) is the most appropriate lawful basis in our

work as Y4H tutors and Trainers, but please see all of the lawful basis's for processing personal data below as set out in Article 6 of the GDPR.

Consent: the individual has given clear consent for you to process their personal data for a specific purpose. See 6.1 below for more details.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations) See 6.2 below for further information.

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

For further guidance see here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#how

6.1 'Consent' Explained

Consent means offering individuals real choice and control. Genuine consent put individuals in charge, builds trust and engagement, and enhances our reputation. At YIHA:

- Individuals are given the option to consent freely, information is specific and unambiguous, and involves a clear affirmative opt-in action.
- Instructions are given to individuals as to how their consent can be withdrawn.
- Data consent requests are separate from other terms and conditions and retained as evidence.
- Personal data collected by YIHA is not shared unless the individual has openly and consciously given permission to do so, which is evidenced through the written consent forms
- There is a separate condition for processing special category data – which includes information about an individual's health (see 5.2).
- Consent forms are kept under review and refreshed if legislative changes require it.
- Records are maintained detailing what data is held, how and why the data is held
- Electronic marketing tools, such as Jot Form, Mail Chimp and Survey Monkey, are also GDPR data compliant and offer individuals the right to opt in or out/ unsubscribe from YIHA mailings.

6.2 'Legal Obligation' Explained

Under GDPR YIHA can store personal data under the basis of 'Lawful Obligation'. To quote the ICO; "*You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.*" YIHA advises all yoga4health trainees and YIHA Y4H tutors to consider the following requirements.

HM Revenue and Customs (HMRC) require all trading entities to keep financial records for 6 years from the end of the last company financial year that they relate to. HMRC have the right to inspect financial information/ data. This means that YIHA are legally required to retain financial information/ data for 6 years.

In insurance terms, the limitation act provides an injured party with the ability to sue for negligence several years after an incident, in certain circumstances. Insurance providers will stipulate the amount of time that they require records to be retained for so it is important to check policy documents.

All personal data retained by YIHA is stored securely (see section 8).

7. Individual Rights

The GDPR provides the following rights to individuals:

- **The right to be informed:** You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.
- **The right to access:** have the right to access and receive a copy of their personal data, and other supplementary information.
- **The right to rectification:** the UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete;
- **The right to erasure:** the right to erasure is also known as 'the right to be forgotten'; The right is not absolute and only applies in certain circumstances (see exceptions in section 6.2).
- **The right to restrict processing:** Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances
- **The right to data portability:** individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **The right to object:** the UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.
- **Rights in relation to automated decision making and profiling:** The UK GDPR has provisions on:
    - automated individual decision-making (making a decision solely by automated means without any human involvement); and
    - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Further information is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

It is important to remember that these rights are not absolute. In certain circumstances you are required to retain data, for example legal purposes, and this can override individual rights. An example would be where you are required to retain records for HMRC financial reporting (up to 5 yrs.) or due to requirements set out by your insurance provider. You must check this before you respond to a data subject access request. In most cases, you have 30 days to respond to a data subject access request.

Please contact YIHA if you have any questions or support requirements with this.

8. Roles and Responsibilities

YIHA will:

- Ensure that an appropriate framework is in place encompassing relevant roles within the organisation that have responsibility for data protection, including the Data Protection Officer
- Provide training for all staff members and students who handle personal information and ensure access to further guidance and support.
- Provide clear lines of report and supervision for compliance with data protection.
- Have contractual arrangements in place to ensure confidentiality and non-disclosure of personal information.
- Store personal data securely and safely and only retain personal data for as long as needed. This may include storing documents in locked cases and filing cabinets and securing electronic data with encrypted/ password protected systems.
- Have a clearly defined process for safely destroying data
- Carry out regular checks to monitor and assess new processing of personal data and to take account of any changes in processing of personal data.
- Develop and maintain procedures to ensure compliance with data protection legislation, to cover for example:
    - Data protection impact assessment
    - Managing responses to subjects' rights requests
    - Management of personal data breaches
    - Provision of privacy information
    - Training and compliance testing
    - Maintain a record of processing activities.
    - Ensure the organisation complies with its transparency and fair processing obligations in relation to data subjects' personal data

9. The Data Protection Officer

YIHA have an appointed Data Protection Officer (DPO) who is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports directly to the Advisory Board in relation to data protection matters. The Data Protection Officer can be contacted by inserting 'Data Protection' in the subject line and emailing: contactyoga4health@gmail.com

10. YIHA Representatives/ Staff/ Tutors/ Students/ Volunteers Responsibilities

All YIHA representatives will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal data.
- Adhere to contractual obligations regarding confidentiality and non-disclosure of information
- Understand fully the purposes for which YIHA uses personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by YIHA to meet its service needs or legal requirements.
- Ensure all personal data is stored safely and securely
- Ensure all persona data is destroyed (in accordance with data collection legislation) when it is no longer required
- Immediately notify YIHA Data protection Officer on receipt of any request for a data subject's information and rights in relation to their personal data
- Not send any personal information without the authority of the Data Protection Officer.
- Understand that breaches of this Policy may result in disciplinary action, up to and including dismissal.

11. Unlawful Obtaining of Personal Data

Section 170 (1) of the Data Protection Act 2018 states it is an offence for a person knowingly or recklessly:

- to obtain or disclose personal data without the consent of the data controller*.
- to procure the disclosure of personal data to another person without the consent of the controller, or
- after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

* the term data controller refers to the application of responsibility for the security of data. As YIHA collect and store personal information, they are, by definition, data controllers.

12. Distribution and Implementation

This document will be made available to all YIHA staff, representatives, volunteers, tutors and anyone representing the YIHA. Anyone representing the YIHA who requires training in data protection and GDPR compliance may request this by inserting 'Data Protection' into the subject line and emailing: contactyoga4health@gmail.com

13. Monitoring and Impact Assessing

Compliance with the policies and procedures laid down in this document will be monitored via the Quality and Standards Manager who will also monitor, review and update this document on a yearly basis or sooner if the need arises.

14. Associate Policies/ Guidance

YIHA Data Protection Guidelines

Contactyoga4health@gmail.com **Tel 07782 413 146**

Charity Number: 1190806

Data Protection Policy

YIHA Data Protection Privacy Statement

YIHA Data Consent Form

Change Record

Date of Change:	Changed By:	Comments:
02.12.2022	AJC	Revised for YIHA purposes.
02.12.2022	PF	Approved
30.11.2023	AJC	Reviewed for currency
06.05.2024	AJC	Reviewed and updated
15.05.2024	PF	Approved

Contactyoga4health@gmail.com **Tel 07782 413 146**

Charity Number: 1190806

Data Protection Policy

Appendix 1: The special category conditions listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) 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;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or 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;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as 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 Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or 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