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

Charity Number: 1190806

Data Protection Guidance

1. Introduction

Data Protection Legislation is applicable to any activity where you are gathering personal data and information about students, service users or other individuals as a tutor, student, member of staff/ volunteers or Y4H tutors. Data processing is also an integral part of any yoga Y4H tutor's role, as students/ service users personal information is gathered to inform Y4H sessions and health and safety practices. YIHA gathers personal information via student and staff data systems as outlined in YIHA Data Protection Policy and YIHA Privacy Statements.

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.

The way in which YIHA meets its legislative requirements is set out in YIHA Data Protection Policy. In addition, YIHA have set out the following data protection guidance to support students, Y4H tutors, staff and volunteers in their roles but this information is not exhaustive.

If you collect personal data you are responsible for ensuring that you comply with the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018. To that end YIHA advises you to take time to ensure you are GDPR compliant and to protect yourself against any legal liability by referring to the Information Commissioners Officer (ICO) via the link below:

1.1 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Summary guidance for practitioners is also available in Appendix 2.

2. Defining 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.

If you collect information about individuals for any reason other than your own personal, family or household purposes, data protection legislation and regulations apply to you and you will need to comply with laws on 'processing personal data'.

The UK data protection regime is set out in the Data Protection Act (DPA) 2018, alongside the UK GDPR (outlined below). It takes a flexible, risk-based approach which puts the onus on you to think about and justify how and why you use personal data.

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

Charity Number: 1190806

Data Protection Guidance

3. 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. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Adherence to these key principles is fundamental to good data protection practice both on an organisational level, such as with YIHA, and on an individual level with regards to Y4H tutors who collect data from their service users, and these principles are essential to complying with the detailed provisions of the UK GDPR. The seven key principles (as outlined by the ICO via the link 1.1 on page 1) are:

Lawfulness, fairness and transparency: data should be processed lawfully, fairly and in a transparent manner in relation to individuals

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: you 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. You must have appropriate measures and records in place to be able to demonstrate your compliance.
More information is available at the Information Commissioner's Office (ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

4. UK GDPR Terminology

Understanding how you are processing 'personal data' is critical to understanding how the UK General Data Protection Regulation relates to your working/ business activities.

4.1 Personal Data

'Personal data' means information about a particular 'identified' or 'identifiable' living individual (see 4.3 below). This might be anyone, including a customer, service user, 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 gathered:

- 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 user 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'.
- Only includes paper records if you plan to put them on a computer (or other digital device) or file them in an organised way, such as maintaining service user/ 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.

See here for further information on personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#3

Personal data relating to criminal convictions and offences are not included as special category data, but similar extra safeguards apply to its processing (see GDPR Article 10). See here for further information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

4.2 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.

Special category data includes personal data revealing or concerning the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

Completion of health questionnaires containing medical data is considered special category data and so this must be considered when you are capturing student/ service user sensitive information via intake forms or other recording methods.

In order to lawfully process special category data, you 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 our Y4H tutors (see Section 6).

It is therefore vital that you obtain express consent, in writing, from all your service users that you have their permission to process their personal health data (see YIHA data consent form on Box).

More information can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

4.3 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 you are gathering/processing. 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

4.4 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 user 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 (CCTV).

5. GDPR Legal Obligations

The UK GDPR applies to personal data and information **'controllers'** and **'processors'** as outlined below. Specific legal obligations are defined within the UK GDPR for processors and controllers for example, processors are required to maintain records of personal data and processing activities, whilst controllers are required to ensure that their contracts with information processors comply with UK GDPR. Processors and controllers have a legal liability if they are responsible for a breach in relation to personal information and the UK GDPR (see section 10).

5.1 What is a controller?

A **'controller'** determines how and why to collect and use personal data. This will usually be an organisation, but can be an individual (e.g. a sole trader/ tutor/ Y4H tutor). If you are an employee acting on behalf of your employer, the employer would be the controller.

For example, YIHA is a data controller. It defines the purpose and methods for capturing student information such as through registration forms and decides what personal data should be collected about which students based on a contractual agreement between YIHA and the data subject (the student). YIHA also gathers information about its employees, volunteers etc. and has a direct relationship with its data subjects (students/ staff/volunteers members). Similarly, Y4H tutors are data controllers as they capture their service user's personal information, with whom they have a direct, contractual relationship. They decide what data is to be collected and how the information will be stored and processed.

In summary: If you exercise overall control of the purpose and means of the processing of personal data, i.e. you decide what data to process and why – you are a controller. The controller must make sure that the processing of that data complies with data protection law.

If you process personal data electronically you may need to register with the Information Commissioner's Officer (ICO) and pay a data protection fee use the ICO self-assessment tool to establish whether this applies to you: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

5.4 What is a processor?

A **'processor'** is responsible for processing personal data on behalf of a controller. Processors follow instructions from someone else regarding the processing of personal data and are given the personal data by a customer or similar third party, or told what data to collect. Processors don't decide to collect personal information or what personal information should be collected from individuals and do not decide the lawful use of that data (as controllers do). Processors do not decide whether to disclose the data or how long to retain the data, they may make a few decisions on how the data is processed but have no interest in the end result.

An example would be the use of third-party software such as survey monkey or mail chimp to gather student/ service user information. The third-party software is the processor and these electronic systems have their own data protection policies.

If you don't have any purpose of your own for processing the data and you only act on a service user's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data.

6. Lawful Basis to Process Data

You must have a valid lawful basis in order to process personal data. YIHA believe that item 'clear consent' from the service user (as listed below) is the most appropriate lawful basis in our work as Y4H tutors, but please see all of the lawful bases 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 should put individuals in charge, build trust and engagement, and enhance your reputation.

- Consent must be given freely, be specific and unambiguous, and involve a clear affirmative action, such as an opt-in. Don't use pre-ticked boxes or any other method of default consent.
- If you wish to rely on GDPR consent you must be able to demonstrate that you have consent, and the individual must be able to withdraw consent easily.
- Provide instructions to individuals as to how their consent can be withdrawn.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough. Be clear and concise
- Name any third-party controllers who will rely on the consent.
- Keep evidence of consent – who, when, how, and what you told people.
- Remember that service user consent to Yoga is not the same as GDPR consent.

- The personal data that you collect should not be shared unless the individual has openly and consciously given you permission to do so and you have evidence of this (written consent).
- Note that if you are processing special category data – which includes information about an individual's health – it isn't enough to just identify a lawful basis for processing. You also need to satisfy a separate condition for processing special category data (see 6.2 below).

Example of how this relates to practices as a Yoga Y4H tutor or YIHA Tutor:
YIHA have created a data consent forms for you to use and these are available on Box.

Make your data consent request prominent, concise, separate from other terms and conditions and easy to understand, i.e. Have a separate consent form for service users/ students that includes:

- the name of your organisation;
- the name of any third-party controllers who will rely on the consent;
- why you want the data - the lawful basis for the processing i.e. 'consent' to capture personal data to ensure the safe participation in yoga sessions/ training as above
- your intended purposes for processing their personal data - what you will do with it;
- how the individuals can withdraw consent at any time.

In addition you should:

- Ask service users/ students to actively opt in with a tick box and signature.
- Keep the service user/ student consent forms as evidence– who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose and give instruction as to how they can withdraw within the consent form
- Keep consent forms under review and refresh them if anything changes.
- Keep a record of what, why, how, where you hold data.
- Only send marketing emails to those that have explicitly 'opted in' to receive marketing and include 'unsubscribe' options for all marketing emails
- Blind copy (BCC) all group emails to prevent sharing email addresses without consent

(see YIHA data consent form on Box).

Note that if you use electronic marketing tools, such as Jot Form, Mail Chimp and Survey Monkey, they are already GDPR data compliant and offer individuals the right to opt in or out/ unsubscribe from your mailings.

6.2 'Legal Obligation' Explained

Under GDPR you 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.*"

HM Revenue and Customs (HMRC) require sole traders to keep financial records for at least 5 years after the 31st January submission deadline of the relevant tax year. HMRC may check this data. HM Revenue and Customs (HMRC) also require all trading entities to keep financial records and have the right to inspect financial information/ data relating to the previous 6 years. This means that you are legally required to retain financial information/ data for the period that applies to you.

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. Under the limitation act it suggests 3 years for someone to be able to bring a claim for injury, from the date they are injured, and in some cases from the date they realise they are injured.

Taking this into consideration you may have reason to retain identifying records (such as student enrolment/ service user intake forms) that could be related/referred to in reference to an injury claim for a significant period after an individual has stopped attending your sessions. YIHA recommend that you review your insurance policy, as it will most likely be a condition of your policy to retain service user records for a certain period of time. See YIHA Data Protection Policy for more information regarding this.

Any retained forms must be stored securely and used only in relation to an insurance claim i.e. information cannot be used for ingoing general communications/use.

7. Individual Rights

Information that you supply to individuals (service users/ students) about the processing of their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

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 section 6.2 above and section 9 'storing and destroying data' below).
- **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/

8. Privacy Notice – what you need to tell people

When processing personal data, you must tell people what you are doing with it. They have the right to know why you need it, what you'll do with it and who you're going to share it with. You should provide this information in a clear, open and honest way. The ICO call this a Privacy Notice and suggest that this is provided to service users/ students when they submit/ complete personal information forms or data collection processes. This applies whether you collect the personal data directly from the individual or you collect their data from another source.

The ICO suggest the following contents to your privacy statement:

- What information is being collected and by whom
- How and why is it being collected
- Information about your lawful basis for collecting the data (or bases, if more than one applies)
- How the data will be used
- Who will it be shared with
- How long it will be retained
- How the data subject can withdraw consent

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/right-to-be-informed/#provide

The ICO example of a privacy notice is available here: https://ico.org.uk/for-organisations/make-your-own-privacy-notice/

9. Storing and Destroying Data

Personal data must be stored securely and safely and you should only retain personal data for as long as you need it. If you hold paper records containing personal data you should ensure that the documents are kept safe at all times to avoid data breaches (see Section 10). This may include storing documents in locked cases and filing cabinets. If you store electronic data these should be secured under a password protection system, such as locking your laptop with a pin code and password protecting data documents, remote wipe facility on phones and tablets and anti-virus software/firewalls. Also consider where the data is stored / backed up. If you use cloud services consider their safety and security, check their policies, e.g. Google Drive, Dropbox – in almost all cases they will have GDPR compliant policies

Whether you're a small organisation, a group or a sole trader that creates or deals with data, you'll also need to have a plan in place for getting rid of this data, either because you've finished your contract with a customer or service user, or a person contacts you specifically to ask for their data to be deleted.

Shredding is a common way to destroy paper documents and is usually quick, easy and cost-effective. Many retailers sell shredders for use within your office or premises, enabling you to shred and dispose of the documents yourself. If possible, consider recycling your shredded documents, as long as you can do this without leaving the data easily available to others during that time.

For more information see here: https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/practical-methods-for-destroying-documents-that-are-no-longer-needed/

The deletion of personal data is an important activity in data protection, given the fifth data protection principle's requirement that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes". In some cases an organisation may be required by law to delete an individual's personal data. The ICO's Personal information online code of practice says: *"It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it. If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way, for example, by accessing a URL from that site. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not."* Remember there are exceptions to the requirement to delete personal data as outlined in section 6.2.

For more information on deleting data see here:
https://ico.org.uk/media/for organisations/documents/1475/deleting_personal_data.pdf

Please note that if you receive a request for right to erasure of data, you are able to refuse if it breaches compliance with a legal obligation – please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ for more information.

For data protection guidance related to COVID-19 see here: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-six-data-protection-steps-for-organisations/

10.Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach of personal data could include loss of student/ service user records in a hard copy folder or allowing unauthorised personnel access to electronic copies of student/ service user data. A common data breach is one where an individual sends a group email without the recipients consent to share their email address. For this reason it is best practice to blind copy (bcc) group emails.

You need to be aware of the guidance around what to do if you suffer a 'data breach' (i.e. misplacement/loss/sharing/hacking of data) and plan for such circumstances. Generally, as a means of good housekeeping you should spend some time thinking about (and document where possible) your personal risk areas in terms of data breaches, how you can alleviate/minimise them and what steps you would need to take if they happened. More information is provided here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/

11.Data Audit

A periodic data audit is sensible as it provides an audit trail that evidences that you have considered and reviewed Data Protection issues. This could be a simple log, that is reviewed annually, showing:

- source of data
- nature of data
- purpose
- IT programmes its used for
- how processed and stored
- who has access
- how it is secure
- retention / deletion policy

12.Appendices

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

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

Charity Number: 1190806

Data Protection Guidance

Appendix 2 Summary Guidelines for Students, Tutors and Y4H tutors

1. If you are (or have previously) collecting, storing and communicating using personal data i.e. names, address, contact details, intake forms/ health questionnaires, you must have permission from the individual to do so.
2. You must provide an explanation as to why you are collecting and storing their personal data and what you intend to do with it. The individual must then consent to say that it is OK for you to do so. See example consent form on Box.
3. Any data that is collected/stored/used must be deleted/destroyed once it is no longer needed (see Section 6).
4. You need to keep a record of what, why, how, where you hold data.
5. Only collect and store data that you really need. Review your data collection forms and ensure that everything you are asking for is required.
6. All personal data must be kept safely and securely. Any paper copies should be securely locked away and any electronic devices containing personal data should be password protected. Wherever possible carrying paper copies of personal data (e.g. intake forms) to and from classes should be avoided due to the risk of leaving them in a public place.
7. Wherever possible data should be carried in a password protected device and/or limited to the essential data that is required in case of emergencies.
8. The personal data that you collect should not be shared unless the individual has openly and consciously given you permission to do so and you have evidence of this (written consent).
9. You need to think about how you do/will store your data so that you can: - Know when you collected it and if you should still have it - Find individuals and delete/update as necessary - Share a copy of the data you hold with an individual
10. Under GDPR, individuals have a right to request to see what data you hold on them (you have a month to comply), the right for their details to be changed if they are wrong and the right to erasure. There is also the right to be informed (covered by the 'Privacy Notice'), the right to object (i.e. if an individual asks you to stop emailing them about your classes you must) and the right to data portability.
11. You need to be aware of the guidance around what to do if you suffer a 'data breach' (i.e. misplacement/loss/sharing/hacking of data) and plan for such circumstances. Generally, as a means of good housekeeping you should spend some time thinking about (and document where possible) your personal risk areas in terms of data breaches, how you can alleviate/minimise them and what steps you would need to take if they happened.

* There is an exception to the above guidelines if the data that you are storing is required in order to meet HM Revenue and Customs (HMRC) requirements. HMRC have the right to inspect financial information relating to the previous 6 years and require all trading entities / sole traders to keep financial records for this length of time. If you are storing personal data for HMRC purposes you must only store the specific data that is required for this purpose and must not use the data for any other purpose.

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

Charity Number: 1190806

Data Protection Guidance

Change Record

Date of Change:	Changed By:	Comments:
Created	AJC	02.12.2022
Approved	PF	02.12.2022