

**DATA PROTECTION POLICY**

*HollyTree Yoga and Wellbeing Services* has to keep personal information as part of the running of it’s weekly classes and services. In doing so the Community Interest Company (henceforth the ‘CIC’) aims to respect the privacy and human dignity of all its practitioners, service users and volunteers at all points throughout the organisation and as far as possible on the basis of informed consent.

The CIC aims to minimise personal data held and only collects personal data for justified reasons and specified purposes. Access to personal data is through strict and formal 'need to know' procedures.

The CIC is registered under the Data Protection Act 1998, registration number Z7376666.

1. **PRINCIPLES**

There are eight data protection principles that are central to the Act. The CIC and all the members of the organisation must comply with these principles at all times in it’s information-handling practices. In brief, the principles say that personal data must be:

1. **Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.** The conditions are either that the practitioner, service user or volunteer has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the practitioner, service user or volunteer, and consists of information relating to:

• race or ethnic origin

• political opinions and trade union membership

• religious or other beliefs

• physical or mental health or condition

• sexual life

• criminal offences, both committed and alleged.

**2.** **Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.**

**3.** **Adequate, relevant and not excessive.** The CIC will review personnel files on an annual basisto ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

**4. Accurate and kept up-to-date.** If your personal information changes, for example you change address, you must inform Holly Webb or Ann Marie as soon as practicable so that our records can be updated. The CIC cannot be held responsible for any errors unless you have notified us of the relevant change.

**5.** **Not kept for longer than is necessary.** Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the CIC decides it does not need to hold for a period of time will be destroyed.

**6.** **Processed in accordance with the rights of practitioners, service users and volunteers, under the Act**.

**7.** **Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**. Personnel files/Client files are confidential and are stored in locked filing cabinets. Only authorised practitioners have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised practitioners. Data held on computer will be stored confidentially by means of password protection, encryption or coding, and again only authorised practitioners have access to that data.

**2.0 PROCEDURES**

2.1 Data information, however stored, should be in a manner that will prevent any breach of confidentiality i.e. deleted from the hard drive/shred written documents.

2.2 Practitioners/Volunteers will be entitled access to their own personal files by gaining permission from Holly Webb or Ann Marie Hall after giving 24 hours notice.

2.3 All written documentation should be stored in a locked filing cabinet at all times. Registers containing personal information needed for sessions should not be left unattended and is only to be seen by the volunteer assisting with the specific session. Registers are then removed from the transport vehicle and kept inside the facilitators home in a locked cabinet.

2.4 Computers holding personal data should be logged off or closed down when the authorised user leaves the workstation.

2.5 Directors are to ensure that all practitioners/volunteers are aware about security systems and procedures during their induction.

2.6 HollyTree Yoga and Wellbeing Services does not use “cookies” on its Website to ensure that no personal data is stored or accessed when browsing the website.

**3.0 EXEMPTIONS**

3.1 There are some exemptions from certain rights and obligations under the Data Protection Act 1998 and subsequent amendment to this Act under the Freedom of Information Act 2000; these relate to:

a) national security

b) crime and taxation

c) health, education and social work

d) regulatory authority

e) journalism, literature and art

f) research, history and statistic

g) information available to the public by or under enactment

h) disclosures required by law or made in connection with legal proceedings

i) domestic purposes

j) written career plans

k) negotiating intentions

I) references given in confidence by an individual's current employer

Exempted data will not be withheld from an practitioner/volunteer when it is for the purpose of obtaining legal advice or otherwise establishing, exercising or defending legal rights.

1. PRACTITIONERS OBLIGATIONS IN RELATION TO PERSONAL INFORMATION

You should ensure you comply with the following guidelines at all times:

* Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this
* Practitioners must maintain records and obtain and share information with parents and carers, other professionals working with the child, and the police, social services as appropriate, to ensure the safe and efficient management of the services, and to help ensure the needs of all children and young people are met.
* Practitioners must enable a regular two-way flow of information with parents and/ or carers.
* Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
* Only transmit personal information between locations by e-mail if a secure network is in place, for example password is used for e-mail. When travelling to and from locations ensure mimimal data is taken out and that it is kept safe to the best of the practitioners ability.
* if you receive a request for personal information about another practitioner, you should forward this to Holly Webb and Ann Marie Hall who will be responsible for dealing with such requests.
* Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected.
* Compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, please speak with Holly Webb or Ann Marie.

The CIC will respond in a co-operative and timely way to all enquiries, notices and assessments issued by the Office of the Data Protection Commissioner.

**5. Physical (Paper) Records**

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

Make sure that there is no other option available to you

Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable

Take only as much as necessary and only for as long as necessary

Transfer it back to its normally secure location as soon as possible

Take all reasonable precautions to keep the records safe and secure e.g.

* Keep them with you whenever possible; lock them away securely when you can’t
* Use a suitable container that prevents accidental loss and/or viewing by others
* Never leave them in plain sight in public places
* Report loss/theft immediately

**6.0 Mobile Storage Devices**

If you are taking data with you on a mobile storage device, such as a tablet PC, laptop, mobile phone, or a USB memory stick, ensure that they are password protected or stored in a locked cabinet:

* Make sure that there is no other more secure option available to you
* Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible
* Keep the password securely and separately from the device/data
* Take all reasonable precautions to keep the device and data safe and secure e.g.

Keep it with you whenever possible

Lock it away securely when you can’t

Never leave it in plain sight in public places

Never let others use your access or device

Delete the data from the device as soon as possible

Report loss/theft immediately