# Hereford Yoga CIC

## Cyber Security Policy

Hereford Yoga CIC has a responsibility to protect all information about our business, particularly personal information held on our students but also information about our staff, suppliers, our financial situation and our business generally.
Our obligations are defined by the GDPR law of 2016 which defines that all holders of personal information must fulfil. The framework for data protection under this law is:

- Understanding what personal data that we hold and what we use it for
- Customers and staff know that we hold personal data and understand how it is used
- Personal data is only collected that is necessary and only kept as long as it is needed
- Personal data is accurate, up to date and secure
- People can exercise their rights regarding the personal data we hold about them
- All staff, including the Board and volunteers know our data protection responsibilities

It follows that Hereford Yoga CIC, to ensure that compliance with GDPR needs to ensure that at all times

- It is registered with the Information Commissioners Office, (ICO) and pays the annual fee
- Personal data is only available to staff on a need-to-know basis
- A clear distinction is made between data used for marketing purposes and data used to provide information
- Downloading of personal information onto personal devices should be discouraged
- Paper records are kept securely and are regularly culled when no longer needed
- Any personal data no longer required is deleted
- All staff are trained to recognise cyber-security threats and how to deal with them
- It has a data breach plan to report any incident within the 72 hour time frame
- It will comply to subject access requests (SAR)
- Reviews are held on the security of data held by third parties – for example Vagaro, Xero, MailChimp and Google Drive
- Insurance Policies provide acceptable level of cover
- Ensure that consent is given by customers for any image taken of them. Where children are involved, consent is obtained from parent, guardian or teacher

In addition to complying with GDPR, Hereford Yoga CIC needs to maintain its defences against cyber-attacks which may aim to disrupt our business and or seek ransom payments

Implications for HYCIC

This is relevant to anyone who is granted access to the Google drive and any other cloud-based system used by HYCIC including Vagaro and MailChimp and should be taken to include all employees/ contractors/volunteers/board members who must

- ensure access to any data that may be considered sensitive or personal is limited to those who need to use it

- If any data is downloaded it should have personal details deleted

- regularly check their own files, as well as those on the Google drive, to check that any data is that is not immediately necessary is deleted

- should ensure that they are aware of the risks posed by
    - Spoofing – acting on email or other instruction that appears to be from a known contact
    - Phishing – being tricked into providing sensitive information or installing malware
    - Fraud – transferring money to wrong account
    - ⇨ If in any doubt, use the phone

- All are strongly encouraged to use best IT practice
    - Keep updating operating software on all devices
    - Maintain anti-virus software
    - Be aware of data leaks that might affect you – for example Vodafone data breach
    - If in doubt, check the website "have I been pwned"
    - Always use strong, different passwords – consider using a reputable password manager
    - Always use 2 factor authentication – don't take the option to "trust this device" or "remember me for 10 days"
    - Be aware of the risk of using free wi-fi, computers with shared access, or giving outsiders guest access to any service
    - Exercise care in downloading any stock image or free software from unknown source
    - Where possible keep personal devices with you at all times – don't leave laptops in cloakrooms
    - Use Credit Card rather than Debit Card when making internet payments
    - Report any suspected breach to Jenny-May immediately
    - Use cloud based back-up services

- Additional Board Responsibilities; to ensure that there is adequate insurance cover and to review this document annually

First Version created 12-03-2023
Amended with Implications 30-06-2023