General Data Protection Regulation (GDPR) Policy and Procedures for Hours of Human Happiness (3H)

### 1. Data protection principles

3H is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
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;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
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 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; and
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.”

### 2. General provisions

1. This policy applies to all personal data processed by the charity.
2. The Trustees jointly take responsibility for the charity’s ongoing compliance with this policy.
3. 3H has registered with the Information Commissioner’s Office as an organisation that processes personal data.

*Karen Whitaker is the contact registered with ICO*

### 3. Lawful, fair and transparent processing

1. To ensure its processing of data is lawful, fair and transparent, the charity shall maintain a Register of Systems.
2. The Register of Systems shall be reviewed at least annually.
3. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

*As we hold such minimal data any requests can be made by email or in writing and will be responded to within 28 days as required.*

### 4. Lawful purposes

1. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the charity’s systems.

*We hold data by consent – our Privacy Policy is on our website*

### 5. Data minimisation

1. The charity will ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

*We have minimised the information held and will continue to do this.*

### 6. Accuracy

1. The charity will take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

### 7. Archiving / removal

1. To ensure that personal data is kept for no longer than necessary, the charity will delete it when requested or when contact with the charity ceases.

### 8. Security

1. The charity will ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions are in place.

*The data is held on personal laptops.*

### 9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity will promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO.

*Everyone should be aware of potential breaches and take appropriate care:*

1. *There are lots of small ways data can accidentally be breached, or be put at risk of a breach. For instance:*

*someone can accidentally cc an email that should have been bcc’d (addresses hidden)*

1. *someone tries to do something good by sharing data but hasn’t checked permissions and consent for this new use*
2. *out-of-date software can ‘leak data’ meaning it sends data around the internet in ways that aren't considered secure any more*
3. *the wrong link can be sent to the wrong person*
4. *malware has got into your systems*
5. *someone has been the victim of a phishing attack.*

*To lower risk:*

1. *check and update systems regularly*
2. *make sure data is not shared*
3. *make sure all trustees and volunteers know how to report a breach (however minor the risk)*
4. *Any breaches should be reported to the Board via email as soon as possible*
5. *The Board will heck whether the breach meets the rules that mean you must report it to the ICO within 72 hours of being made aware of it.*
6. *The ICO small organisation helpline is there to help (0303 123 1113).*

Register of Systems

|  |  |  |
| --- | --- | --- |
| System | Information held | Archived |
| List of sponsors – used to send newsletter | Name, email address | Until sponsorship ceases |
| List of Giftaid sponsors | Name, address, consent to Giftaid | As required by HMRC |
| List of individual beneficiaries | Name, phone number | Until sponsorship ceases |
| List of donors – used to send newsletter | Name, email address | Until advised they no longer want newsletter |
|  |  |  |
|  |  |  |

Drafted by KW on 15.3.19 and updated 27.3.24