GDPR Compliance Statement - May 2018

1. Background

YHA acts as both a Data Controller and a Data Processor, and has taken significant steps in the past 18 months to ensure it is fully compliant with the General Data Protection Regulation (GDPR).

This GDPR Compliance Statement sets out YHA's approach to managing personal data as part of its risk management process. It provides assurance of YHA's GDPR compliance in relation to the personal data of all YHA contacts, including: potential, existing and previous customers, supporters, employees, corporate contacts, partners and suppliers.

2. GDPR compliance actions

YHA has taken the following actions to ensure it is GDPR compliant by 25th May 2018:

- **All YHA personal data has been audited** to record the data we hold, where it comes from and who can access it, and where it is stored, and has clear and documented ownership, retention periods and confirmed lawful basis for processing – which have been verified by our third party compliance advisers.

- YHA has a **Data Protection Policy** which includes detailed guidance for all employees about how to obtain, store, use, process, secure, transmit and destroy personal data in compliance with the GDPR.

- YHA's **Privacy Policy** is published on the footer of its website, and is regularly updated to reflect the measures taken by YHA in relation to personal data.

- Other **data privacy-related policies and processes** are in place to meet the requirements of the GDPR, including: Data Retention Policy; Privacy Policy; Information Security Policy; Subject Access Request process, Incident Response Plan; IT Policy; Data Privacy Impact Assessment process; CCTV Policy and Information Classification

- **Privacy by design** is an integral part of YHA's project and change management processes, to ensure that data privacy is considered at the outset of any processes or procedure development

- **GDPR training** has been developed and delivered for all YHA employees; this training will form part of new employees' induction to YHA, and refreshed training will be undertaken annually.

- **Appropriate controls** are in place to ensure that data is only accessed as necessary by authorised YHA personnel.

- YHA has **physical controls** to ensure that all electronic data is secured to prevent it from being externally accessed.

- YHA has an **Incident Response Plan** with breach protocols that meet GDPR requirements; this identifies named individuals that are accountable in the event of a breach, and holds information about how relevant parties will be informed in event of a data-privacy related incident

- Where appropriate, **external suppliers and partners** have the necessary contractual arrangements with YHA in place to ensure they are GDPR compliant.

- YHA achieved **PCI-DSS compliance** in November 2015. YHA does not store credit/debit card details on our systems, and therefore the risk of cardholder data breach is low. This is now audited annually.

3. Obtaining and processing personal data

- YHA obtains and processes personal data in accordance with the GDPR and historically, the Data Protection Act 1998, using one or more of the six lawful bases for processing as stated in the GDPR.

- YHA does not sell personal data to any third parties under any circumstances, and will only share it with organisations we work with when its necessary and the privacy and security of the data is assured.

4. Storing personal data

- YHA does not store data for longer than necessary; **data retention periods** are in place, and data owners are managing the destruction or anonymization of data once this retention period has ended.

- **YHA stores personal data** both on its network at the YHA National Office in Matlock, and at an external Data Centre in Derby, that is specifically designed for this process. This facility is PCI-DSS and GDPR compliant.

- YHA may on occasion store data outside of the **European Economic Area** and when doing so ensures that appropriate security measures are in place. For all contracts of this type, specific contractual arrangements are needed to ensure that the data is stored in compliance with GDPR.

- YHA does not store **customer credit or debit card details** on any of our systems regardless of where they are hosted. Where card payments are taken, these are processed and transmitted using third party systems which are compliant with PCI-DSS.

5. Technical Security Measures and compliance

- All staff are required to read and adhere to the **ICT Acceptable Use Policy**

- All laptops, PC's and Thin Clients are **password protected**

- All laptop hard drives are **encrypted**

- Smartphones are secured by a **pin number** if not accessed for 1 minute

- **Backups** are stored on a Network Attached Storage Device which is stored in an externally owned secure PCI-DSS/GDPR compliant Data Centre in Derby and further backup is stored at YHA's National Office in Matlock.

- YHA maintain **firewall** with an active/passive configuration any changes are logged and checked in a change management log

- We have a data privacy and systems **Incident Response Plan** to detect, report and investigate a personal data breach, which is tested and reviewed annually

- YHA have **annual penetration testing** undertaken by a third party to test the security of its systems.

- **YHA websites** are automatically updated by the hosting providers who will ensure it is up to date with all security patches.

- **Antivirus programs** are installed on all IT servers and laptops and are automatically updated

- **National Office** is secured with key card access controls preventing unauthorised entry

- Our **server rooms** are monitored with CCTV, and access to this area is tightly controlled for authorised personnel only using Key Card Access Controls

- **Regular maintenance** of our ICT infrastructure is carried out and security patches are applied in a regular and timely manner

- All YHA systems have appropriate technical security controls (eg encryption, verification, authentication and access controls) relative to the type of data stored.

6. Contacts and links

- YHA's Privacy Notice can be viewed at www.yha.org.uk/privacy

- YHA is registered with the UK's regulator the Information Commissioner's Office (ICO) – Registration Number: Z6434257

- The ICO's website can be viewed at www.ico.org.uk

- YHA's Data Protection Team can be contacted
    - by email at dataprotection@yha.org.uk
    - by writing to us at:

      Data Protection Team
      YHA (England and Wales)
      Trevelyan House
      Dimple Road
      Matlock
      Derbyshire
      DE4 3YH