Data Protection Compliance Statement

1. Background

YHA (England and Wales) is registered with the ICO (Z6434257) and processes personal data in order to deliver accommodation and other services. Our Privacy Notice sets out the detail of our processing. This Data Protection Compliance Statement sets out YHA's approach to managing personal data as part of its risk management process. It provides assurance of YHA's compliance in relation to data protection legislation.

This statement was last updated on 20 December 2022.

2. Compliance actions

YHA takes the following measures to ensure compliance with data protection legislation:

- **All YHA personal data is audited** periodically to ensure we meet the accountability requirement of the UK GDPR and understand what data we hold, our processing purposes, permissions for use and retention periods.

- YHA has a **Data Protection Policy** which provides guidance for all staff on the appropriate use and management of personal data held by YHA.

- YHA's **Privacy Notice** is published on the website and is periodically updated to reflect any changes in our processing.

- Other **data privacy related policies and processes** are in place to support staff in secure and effective data management, including our Data Retention Policy; Information Security Policy; Data Rights process, Incident Response Plan; IT Acceptable Use Policy; Data Privacy Impact Assessment process; CCTV Policy, Register of Processing Activity and an Appropriate Policy Document covering our processing of Special Category and criminal data.

- YHA takes a **data protection by design and default** approach to ensure that data privacy is considered at the outset of any new project or service which includes personal data processing, or where an existing project or service changes, so we can identify and manage may risks to data subjects.

- **Data Protection training** is mandatory for all staff, including induction training for new starters, annual refresher training and specialist or topic training according to role, to ensure staff understand and maintain awareness of the legislation, our policies and how these apply to their work.

- **Appropriate security controls and protocols** are in place to ensure that data is only accessed by authorised individuals. 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; this includes named individuals who are responsible for managing breaches, the plan holds information about how relevant parties will be informed in event of a data-privacy related incident

- **External suppliers and partners** have contractual arrangements in place to ensure the appropriate management of personal data on YHA's behalf and any transfers outside the UK are managed with appropriate safeguards in place.

- YHA achieved **PCI-DSS compliance** in November 2015 and re-confirms compliance annually. We do not store credit/debit card details on our systems, and therefore the risk of cardholder data breach is reduced.

- YHA has a **Data Privacy Stewards Group**, with representatives from across YHA, with a remit to review day to day processing. An **Information Governance Group** considers data protection, cyber security matters and policy, reporting to the **Risk Management Group** which reports in turn to the **Audit and Risk Committee**, responsibility for data protection ultimately rests with the Board of Trustees.

3. Obtaining and processing personal data

- YHA collects and processes personal data in order to administrate accommodation bookings, provide associated services, manage fundraising activity and generally pursue our charitable objects.

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

4. Storing personal data

- **Data retention periods** are in place, and data owners manage the secure disposal or anonymisation of data once its retention period is reached and the data is no longer required.

- **YHA stores personal data** both on our network at the YHA National Office in Matlock, and at an external Data Centre in Derby. This facility is PCI-DSS compliant.

- YHA may on occasion **store data outside of the UK** and when doing so we ensure that appropriate security measures are in place. For all contracts of this type, specific contractual arrangements are in place to ensure that the data is stored securely and in compliance with UK 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 with backups stored at a separate location.

- YHA maintains a **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, this is tested and reviewed annually

- YHA has **annual penetration testing**, undertaken by a third party, to test the security of our systems

- YHA **websites** have up to date security patches applied by the hosting providers

- **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

- YHA **server rooms** are monitored with CCTV, and access to the area is tightly controlled and limited to authorised personnel only.

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

- All YHA systems have **appropriate technical security controls** (e.g. authentication and access controls) relative to the type of data stored

6. Contacts and links

- YHA's Privacy Notice can be viewed at https://www.yha.org.uk/our-policies/privacy-policy

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

- The ICO provides guidance on data protection https://ico.org.uk/your-data-matters/

- 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