INFORMATION SECURITY POLICY STATEMENT

Our Commitment to Information Security
In the course of our business activities we collect, store and process a vast amount of information using a variety of methods and communication equipment and we are committed to satisfying all statutory requirements for Information Security. The protection of our information assets is vital to the success of our business. Our objectives for Information Security are that:

- We will establish our requirements for information security and identify our key information assets.
- We will seek to identify the threats to our information assets in order to carry out a documented risk assessment and develop a Risk Management Plan. This will include establishing, documenting, maintaining & testing an effective Business Continuity Plan.
- Documented management control procedures will be implemented to support this policy in accordance with the requirements of BS EN ISO 27001:2013.
- Company personnel will be given adequate training in their information Security responsibilities.
- Sensitive information will be strictly controlled and will only be accessed by authorised personnel to ensure that confidentiality is maintained.
- The integrity of information will be maintained throughout its processing to secure it against accidental or deliberate damage, loss or destruction.
- Suspected breaches or weakness in our Information Security protocols will be reported & investigated.
- The effectiveness of the Information Security Management System will be continually reviewed and improved to meet our business needs.

Information Processing
Obtaining, recording, holding, or working with information will be carried out in accordance with the requirements of our documented policies and procedures. This includes the organising, amending, retrieving, using, disclosing, transmitting, erasing or destroying of information. This applies to all forms of information including information in hard copy, electronic or verbal form.

Personal and sensitive personal data
All personal or sensitive data including CCTV images are subject to the Data Protection Act 1998 and will be controlled in accordance with the Company's Data Protection Policy.

Implementation
Managers at all levels are directly responsible for implementing this policy and for ensuring staff compliance within their respective departments. This policy is not part of the contract of employment and we may amend it at any time. Any breach of the policy will be taken seriously and may result in disciplinary action. Any employee who considers that this policy has not been followed in respect of Information Security should raise the matter with his or her line manager in the first instance.

Information Security Manager
The Senior Management Team will appoint an Information Security Manager responsible for ensuring compliance with all relevant Information Security legislation and this policy.

Richard Towl
SWH Managing Director
Date: January 2017