INFORMATION SECURITY ASSURANCE POLICY

As a Group we have implemented an Information Security Management System, complying with the requirements of ISO 27001 and Cyber Essentials, to ensure that we assess risks within the business and strive to prevent security incidents.

The scope of this Security Management System includes information stored on computers, transmitted across networks, printed out or written on paper, stored on portable media, or spoken in conversation or over the telephone.

It is our Policy to ensure that:

- We comply with UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.
- All customer, client or Group held data is protected, handled, and shared where necessary in accordance with the requirements of UK Data Protection Laws and and, to the extent applicable, the data protection or privacy laws of the country of the data owner.
- Regular audits and reports which will be reviewed by the **eacs** Board.
- All breaches of Information Security, actual or suspected, are reported and investigated up to Board Level.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory and legislative requirements, together with any contractual security obligations, are met.
- Information is protected against unauthorised access
- Objectives and targets are set and monitored to achieve continual improvement in our Information Security Management System.
- Information Security Training is provided, where required.
- Procedures and instructions are implemented to support this Policy.

All Managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

It is the responsibility of each employee to abide by this Information Security Policy Statement and associated policies.

Clinton Groome

COO