James Lister & Sons Ltd
Spon Lane South
Smethwick
West Midlands
B66 1QJ
Tel • (0121) 553 2411 Fax • (0121) 525 6116
Email • enquiries@lister.co.uk Web • www.lister.co.uk

Information Security Management System Policy

It is the policy of James Lister & Sons Limited to treat all information with appropriate care and security as a means to comply with all statutory, regulatory and contractual requirements, and, to protect the interests, property and information of the company, and of its clients and employees, against threats or loss. This applies to information that is both documented or un-documented, and to hard copy or electronic data.

The purpose of this Information Security Management Policy statement is to describe how security is implemented, to give guidance to our employees whose actions can affect the confidentiality and integrity of the business, its product and services, and, to illustrate the overall commitment to security issues within our company. This policy is underpinned by a range of other Lister policies, procedures, certifications and working practices, which define our company's security activities. These include;
Certification to Cyber Essentials
Lister GDPR Policy (and Customer/Supplier Privacy Notice)
Lister Employee Handbook - Electronic Communications Policy, Social Media Policy
Lister QEHS Management System Manual working practices
Confidentiality clause in Lister employment contracts
NDAs where appropriate

This Policy is maintained by audit and review, and by the methods described in the QEHS Manual, in order to provide effective assurance that all aspects of company, employee and customer specified security requirements are being implemented.

It is company policy to ensure that the use of documents, computers, mobile computing, mobile communications, mail, email, voice mail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorized use and to reduce security risks. Employees are reminded to take suitable care of all data, especially customer related information, and to follow all information security requirements, particularly where confidential information in concerned.

All employees have a responsibility not to compromise the company, e.g. by sending defamatory or harassing electronic mail, or by making unauthorized purchases, and, must also be aware that the confidentiality and integrity of information transmitted by email may not be guaranteed.

Peter Davies
Chief Executive
7 June 2018
Reviewed 12 March 2019, 29 February 2020