

Johnston Mailing ISMS Policy

The Johnston Mailing information security policy provides management direction and support for information security in accordance with business requirements and relevant laws and regulation.

The key aspects are:

- To ensure that information is managed as a valuable asset and is fit for purpose;
- To give greater assurance to Regulators, customers, potential customers, employees, trading partners and stakeholders that information security is being well managed within Johnston Mailing;
- Demonstrate credibility and trustworthiness to these bodies;
- Reduce the risk of losing business or incurring fines due to an information security breach;
- Establish and demonstrate that relevant laws and regulations are being met;
- Ensure that a commitment to Information Security exists and is communicated to all levels throughout the organisation;
- Have a commitment to continual improvement;
- Have a clear set of objectives for information security.

Information Security Objectives

The objectives have been set to enable the effectiveness of the Johnston Mailing ISMS to be monitored and measured on a regular basis.

They are the responsibility of the senior management team and a sample are given below:-

- The ISMS is reviewed and updated on a regular basis
- Risk assessments are carried out at least once per year
- All security incidents are reviewed within 5 working days of being raised
- Security updates will be provided to staff when recognised
- The objectives and their measures will be reviewed by management during their regular meetings which include a review of security
- Management will ensure that sufficient resources are provided to achieve the ISMS objectives

All staff and relevant 3rd parties and sub-contractors are expected to follow the ISMS policy and be made aware of the ISMS's requirements and their obligations to conform to the Johnston Mailing ISMS.

Signed

.....
Scott Johnston

Date 05/02/2025