1 Introduction and Scope

1.1 This policy relates to the Data Protection Act 1998 and to the SES Group internal procedures for processing personal data, including where necessary, consultants and contractors. (See 1.2 below)

1.2 The policy outlines the SES Group obligations and commitment to ensure that individuals' rights are upheld in relation to:

- Confidential, personal and sensitive personal data held either manually or within electronic systems that are utilised for the processing of data relating to Clients, Customers, Board Members, Employees (current and former), applicants seeking employment and relevant suppliers, contractors and data processors.

1.3 The requirements and accountability to compliance with the Data Protection Policy apply to all the SES Group current and former employees, Board Members, Consultants, Contractors or Third Parties contracted to carry out services on behalf of the SES Group where individuals personal data and or sensitive personal data is processed.

The Data Protection Act (DPA) requires that organisations (data controllers) process personal data in accordance with the eight Data Protection Principles.

1.4 The SES Group acknowledge that individuals have the right to expect that suitable, appropriate and reasonable safeguards will be operated by the SES Group and any third parties engaged to protect the confidentiality, integrity and security of their personal and sensitive data.

1.5 Where a third party processes data on behalf of the SES Group we will ensure that the third party also acts in accordance with the DPA. This will be ensured through a legal document.

1.6 The SES Group understand that the consequences for non-compliance of the DPA could result in:

- Personal accountability and liability
- Organisational accountability and liability
- Criminal and civil action
- Financial penalties issued by the Information Commissionaire
- Loss of confidence to the integrity of our systems and processes.
- Reputational damage to the organisation.
- Individuals seeking compensation for damages relating to Data protection breaches
- Disciplinary action

1.7 This policy applies to data held either manually or within electronic systems utilised for the processing of personal and or personal sensitive data. It outlines the SES Group responsibilities and commitment to compliance with the DPA and serves to ensure that individual rights are upheld.

1.8 The Data Protection Act 1998 requires that personal data is processed in accordance with the eight Data Protection Principles detailed below:

- Personal data shall be processed fair and lawfully
- Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and kept up to date.
- Personal data processed for any purpose will not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
- Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Marketing and Promotion of Goods and Services

We will NOT share or sell your data to other third-party organisations for the purposes of marketing or promotion of goods and services.

2.1 The Data Protection Act 1998 is designed to ensure that data controllers meet their obligations and individuals can exercise their rights in relation to the processing of personal data. The Act defines the organisation responsible for processing the personal data as the 'data controller', an individual as a 'data subject' and their personal information as 'personal data', these and other terms are further defined in Appendix 1.

2.2 The SES Group will take all reasonable measures and actions to meet their obligations under the Act as data controllers. We will ensure correct data processing requirements are in place to protect individual's personal data where it is shared with third parties, (data processor) who are acting under our instruction to process individual's personal data on our behalf.

We will ensure personal and sensitive personal data is fairly and lawfully collected in line with individual's rights. In doing so we will ensure Personal and Sensitive Personal Data is collected, processed and shared in line with schedule 2 and 3 of the Act. We will abide by the law to ensure the confidentiality of customers and employee's data and ensure any data sharing is not carried out with unauthorised third parties. When data sharing we will consider any possible adverse effects on the individual(s). The SES Group would only carry out Data Barring Service Checks where permitted by law, when they are required for employment purposes and when they in in the public interest.

3 Policy Statement

3.1 We will adopt and follow this policy and the requirements of the supporting Data Protection, Information Governance and Security Framework(s) and System(s) for those individuals outlined in point 1.2. The core requirements relate to the:

- Collection, storage, processing, records, confidentiality, security, incident management, retention and deletion, management, availability, integrity and secure disposal of personal and sensitive personal data.

3.2 We will only collect and process personal and sensitive data that has been obtained fairly and lawfully and for a specific set of purposes or where we have a legitimate purpose(s) under the law to do so. Data will be adequate and relevant and only used for the purposes collected. It will be maintained, kept accurate with the help of the individual and not retained for any longer than is necessary.

3.3 We will ensure personal or sensitive personal data is processed in line with the law, kept both secure and confidential at all times and ensure all individual's governed by this policy will:

- Only access and process data that they are authorised to on behalf of the SES Group;
- Adhere to all Information Governance, Data Protection, Security, Human Resources frameworks and procedures supporting this policy;
- Only share information with third parties where it is fair and legal to do so and in accordance with published fair processing notices;
- Apply the ICO good practice codes in Subject Access Request, Data Sharing, Privacy Impact Assessments and Employment Practice Code;
- We will adopt the good practice set out by the ICO CCTV code of practice in all our operating systems.

3.4 We will ensure all existing and new employees and Board Members will undertake data protection and security training and as part of this they will be accountable to embed and promote good information handling and security, and apply the 8 data protection principles. All new starters of the Group will undertake training within three months of starting and every 24 months or as and when the law requires.

3.5 We are committed to ensuring that all appropriate technical and organisational measures are taken to prevent against unlawful access, process, accidental loss or destruction of, or damage to personal data we hold.

3.6 We will only transfer personal data to jurisdictions outside the European Economic Area (EEA) if it has a recognised and adequate level of protection for data protection purposes'. Transferring data outside of the United Kingdom requires a Director's approval and relevant Information Governance and Security compliance checks.

3.7 The Managing Director of the SES Group is responsible for reviewing the annual notification and ensure all business areas report changes or new forms of processing to the designated Data Controller who will make the necessary arrangements to notify the Information Commissioner Office (ICO) on behalf of the company Managing Director and they will report this annually to their company board.

The Data Controller or each company should periodically check their registration to ensure it continues to meet all their data processing activities.

3.8 We will comply with all relevant data protection processing, privacy notices and notification to any future acquisition and/or merger with third parties, including for example our obligations under Transfer Undertakings Protection of Employment Regulations. We will ensure that all personal or sensitive personal data is only shared when legally required and anonymised as part of any testing, evaluation of assets and liability assessments except as required by law.

3.9 We acknowledge that individuals have further rights

- To make a request in writing for access to and be provided with a copy of their personal data that they are entitled to receive under the Act. We will apply a £10 fee as defined in the Act and respond to requests within 40 calendar days upon receipt of a formal and valid request;
- To request that their personal data are deleted or corrected if they believe the information is inaccurate, excessive or out of date. We will apply to the applicable requirements of the Act and respond within 21 calendar days of receiving the request;
- To prevent the processing of their data if it is as defined in the Act, causing damage or distress to them, in relation to automated decision making and to opt-out of processing for direct marketing purposes;
- Disclosure of personal and sensitive personal data shall be assessed in line with the exemptions of disclosure as defined in the Act. Individual or Third party data will be deemed confidential and will only be disclosed or shared with consent of the individual and/or where we are legally obliged to under the Law.

3.10 We will ensure that all customers are made aware of our approach and obligations in respect of the Data Protection Act 1998.

3.11 Complaints relating to alleged breaches of the Data Protection Act or complaints that an individual's personal information is not being correctly processed will be managed and processed by the Data Controllers and the Managing Director. All complaints of alleged customer service dissatisfaction will be separately processed in accordance with our complaints procedure after the Data Protection complaint has been fully reviewed and responded to.

3.12 The SES Group may consider taking internal disciplinary or contractual/legal action where members governed by this policy do not comply with this policy, the Data Protection Act 1998 and our associated frameworks, policies and procedures.

4 Information Sharing

4.1 The SES Group will only share personal information in accordance with the principles of the Data Protection Act 1998 and as required by law or regulation. We will only share relevant information with partners and selected third parties who are working on our behalf, or with whom we have a legitimate interest to share individuals' personal information. We will inform individuals how we will process and share their personal information via our privacy policies and fair processing notices. Examples and purposes for sharing information are:

- For the prevention or detection of crime and apprehension or prosecution of offenders
- For the assessment or collection of tax or duty owed to customs and excise, this may include utilities' where a customer owes a debt
- When required in connection with legal proceedings or gaining legal advice
- In relation to the physical or mental health of an individual to protect their and other's interests
- For research purposes
- To comply with the law
- Where it is in our legitimate interests or as part of our legal or regulatory obligations we may receive and share individual personal data. In doing so we will consider if the sharing may prejudice the rights and freedoms or interests of the individual and act accordingly and within the law

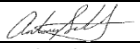
Confidentiality
All current and former employees, board members, supplier and contractors are responsible and accountable for security and confidentiality of company and individuals data they process. A breach of this will be deemed a serious offence. Any person(s) found to share/disclose or obtain data without the consent of the SES Group and are found to have knowingly, recklessly, deliberately or without authorisation breached these instructions or policies renders him/herself liable for disciplinary, contractual and/or legal prosecution in accordance with the SES Group Employment and Supplier/ Contractor obligations:

4 Equality and Diversity

4.1 We will ensure that this policy is applied fairly and consistently. We will not directly or indirectly discriminate against any person or group of people because of their race, religion / faith, gender, disability, age, sexual orientation, gender reassignment, marriage and civil partnerships, pregnancy and maternity or any other grounds set out in our Equality and Diversity Strategy.

5 Review

5.1 We will carry out an annual health check taking account of legislative and regulatory changes and a fundamental review of this policy every two years. Further Advice and Assistance contact the Data Controller.

Name:	Tony Ball
Signature:	
Date:	23/01/2018