FES GROUP OF COMPANIES
DATA PROTECTION POLICY STATEMENT

This document sets out the Company's policy for protecting the "Personal data" that we process i.e. data that can be attributed to an individual and which is either processed automatically, e.g. through a computer, or held on video, or else forms part of a filing system e.g. hard copy records.

We will ensure that personal data is always processed in accordance with the provisions of the Data Protection Act (DPA) and the General Data Protection Regulations (GDPR). It is our policy that all personal data will be:

- Processed fairly, lawfully and transparently.
- Collected for specified, explicit and legitimate purposes and not further processed incompatibly.
- Adequate, relevant and limited to what is necessary.
- Accurate and up to date.
- Kept for no longer than is necessary for its purpose.
- Processed in a way that ensures appropriate security, protection against unauthorised or unlawful processing and accidental loss, destruction or damage.
- Adequately protected when transferring to any other party.

We will put in place the following organisational and technical measures:

- Registration (Notification) with the ICO as a Data Controller.
- Provision of training and awareness to all of our people who are involved in processing personal data.
- Prior to processing personal data we will identify the relevant lawful basis and document it.
- When obtaining personal data, we will either select a "Legal basis" for the processing or obtain consent.
- At the time of collecting personal data, we will communicate a Privacy Notice.
- We will ensure that data subjects rights are upheld at all times
- Restricting personal data access to individuals having legitimate business reasons for processing the data.
- Comprehensive, proportionate governance arrangements for processing activities
- Appropriate technical and organisational privacy protection measures.
- Measures that meet the principles of data protection by design and data protection by default.
- Maintaining internal records of our processing activities.
- Undertaking Data Protection Impact Assessments (DPIAs)/Privacy Impact Assessments (PIAs).
- Although it is not a legal requirement we have chosen to appoint a Data Protection Representative (DPR) who will act as a focal point for data protection issues, uphold and invoke data subject rights and who will interact with relevant supervisory authorities where required i.e. breach notifications and investigations.
- Investigating and reporting certain types of data breach to the relevant supervisory authority.
- Behavioural controls to maintain data subject privacy.
- Adequate supervision to ensure that standards are being maintained.

This policy will be maintained and regularly monitored to ensure that all objectives are achieved. It will be reviewed and revised where necessary to ensure that it remains relevant.

Signed

Duncan K Fletcher
Managing Director
7 January 2019

The management reporting lines are documented in the accompanying FES organisation chart.
The following responsibilities are apportioned throughout the organisation. The people with responsibilities are duly authorised by the Managing Director (and so have his authority) to take the necessary steps to ensure compliance and each person will be held accountable for delivering their responsibilities in practice:

Managing Director.

- The Managing Director has ultimate responsibility to ensure that the company fulfils its legal obligations and to ensure that data protection objectives are set and achieved.
- Ensuring that effective management, financial, human and other resources are employed in the pursuance of the stated aims of the data protection policy.
- Ensuring that policies, the management system and its operation are reviewed regularly to ensure compliance with the law, the business plan of the organisation and to achieve continuing improvement.
- Defining, establishing and maintaining the data protection policy.
- Appointing and empowering a competent and suitable risk management team.
- Communicating and championing the importance of effective data protection management throughout the organisation.
- Considering data protection performance in long-term planning.
- Convening and participation in the management review process which will include the setting of objectives, targets and programmes.

Data Protection Representative (DPR) (Assisted by the Risk & Compliance Team).

- Registering the FES Group companies with the ICO and maintaining registration.
- Ensuring the company is aware of statutory obligations and recommended codes of practice.
- Maintaining and continually improving an Integrated Management System (IMS) which incorporates elements and operational controls necessary to comply with data protection legislation.
- Assisting personnel at all levels of the business in matters relating to data protection.
- Advising management on their responsibilities for incident prevention and the avoidance of risk to data protection.
- Interpreting and updating management and employees on new and developing legislation and other standards.
- Advising through line management where improvements in standards or practices can be made.
- Advising on possible data protection issues where new equipment or changes to working practice is considered.
- Reviewing of all breach investigations and reporting on statistics relating to data protection performance.
- Advising on training programmes.
- Ensuring where requested that all Data Protection Impact Assessments (DPIAs) are carried out by the relevant managers are suitable, sufficient and documented.
- Assisting development the company IMS as it refers to data protection management.
- Auditing managers on compliance with company procedures and preparing reports for the Managing Director on compliance.
- Communicating audit reports to the relevant board members along with recommendations to ensure compliance.

Managers & Directors.

- All are accountable to the Managing Director for the implementation of company policy.
- All are responsible for data protection for all employees for whom they have operational responsibility.
- Responsibility for the implementation and management of the company data protection management system.

- Ensuring that all persons and 3rd parties working for them are properly briefed on their data protection roles and responsibilities and are provided with guidelines to state security expectations of their role within the organisation prior to being granted access to personal information or information systems containing it.
- Ensuring that data protection procedures are developed and adhered to and to ensure that all persons working under their remit including 3rd parties, suppliers etc are suitably trained and to support their efforts on data protection.
- Ensuring that background verification checks are carried out for all candidates for employment, contractors, agency staff and third party users who will have access to sensitive personal data proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
- Ensuring that Data Protection Impact Assessments (DPIAs) for their area of control are complete, suitable & sufficient, up to date and revised in the light of any changes.
- Completing any action on or before the date noted on the Objectives & Targets Programme or in any audit or inspection report or if this is not possible, agree any extension to the timescale with the "Authorised person" for the area of the business in question.
- Identifying of non-conformities and management of preventative and corrective actions relating to their responsibilities.
- Ensuring that all documents & records are complete, up to date, correctly controlled, filed and protected.
- Reporting all significant breaches, near misses etc to the Data Protection Representative (DPR).
- Ensuring that work activities carried out by company employees and sub-contractors do not create uncontrolled data protection risks, hazards or breaches.
- Ensuring that suitable and practical emergency preparedness and response procedures are in place to cope with breaches relating to the identified data protection risks that are within their control.

Managers and Directors are responsible to ensure that the following are provided for the employees and sub-contractors directly under their control:

- Training is carried out and documented.
- Adequate supervision is in place to ensure that standards are being maintained.
- Hazards and risks to data protection are assessed and lowered as far as possible.
- Investigation and documenting all data protection incidents etc and recommend means of preventing recurrence.
- They are fully aware of all data protection working practices and procedures.
- Ensuring that data protection activities carried out by company employees and sub-contractors do not create a risk or hazard to data protection.
- Ensuring that all 3rd parties, sub-contractors and suppliers employed are managed in compliance with the policy and procedures at all times.

All Employees.

Will ensure that:

- They are fully conversant with the data protection policy and comply with it.
- They will co-operate with the company in meeting its statutory duties.
- They will not attempt to carry out any works that they are not competent to do.
- They will protect personal data from unauthorised access, disclosure, modification, destruction or interference.
- They report any inadequacies of company data protection policy to their line manager.
- They will take reasonable care of personal data under their control.
- They do not intentionally or recklessly interfere with or misuse anything provided in the interests of data protection.
- All breaches, near misses etc are reported immediately to their line manager.

- They are fully conversant with the data protection procedures for the area in which they are working.
- All data protection assets are used and maintained in a condition fit for purpose and any defects are reported immediately to management.
- They comply fully with their legal responsibilities and rights.
- Comply with all data protection and information security policies, procedures, guidance etc at all times including when information is being processed outside the organisation's premises and/or outside normal working hours, e.g. in the case of home-working.

The following responsibilities are to be assumed when processing "Sensitive personal information" only:

- A confidentiality agreement is to be signed prior to being given access to information processing facilities.
- Apply the correct classification and implement the specified controls to information.
- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities are adopted.
- Information on paper or on electronic storage media is locked away in a safe or cabinet or other forms of security furniture when not required.
- Computers and terminals are left logged off and protected by password authentication when not attended.
- Unattended facsimile machines are not to be used for those purposes.
- The unauthorised use of photocopiers and other reproduction technology such as scanners, digital cameras etc is prohibited.
- Documents may only be printed to printers which require local log on, will be attended whilst printing is in progress and where the printed documents are removed from the printers immediately by the recipient.

Note that the responsibilities described above will continue to apply for a period of 12 calendar months after the end of the employment.