Group Data Protection Policy

Policy Statement

Each business (each a "Group Company") within the James Fisher and Sons plc group (the "Group") is required to maintain certain personal data about employees for the purposes of satisfying operational and legal obligations. The Group recognises the importance of the correct and lawful treatment of personal data.

Personal data, whether it is held on paper, computer or other media, will be subject to the appropriate legal safeguards as specified by the General Data Protection Regulation ("GDPR"). The purpose of the GDPR is to regulate the way in which personal information about individuals is obtained, stored and can be used, disclosed and transferred. In order to enable each Group Company to satisfy its responsibility for data protection (exercised by the relevant Data Protection Officer), it is vital that all employees who obtain, handle, process, transport and store personal data must adhere to the principles set out in this policy.

This policy sets out your obligations with regard to personal data about other people which you may have access to in the course of your employment. It is your duty to familiarise yourself with this policy, and ensure you understand how it may apply to you in your day-to-day job. Any breach of this policy by you may result in disciplinary action (which may include dismissal) and may constitute a criminal offence.

The potential financial impact of an infringement of GDPR is huge: up to the higher of 4% of annual worldwide Group turnover and EUR20 million. Just as important is the reputational impact of an infringement on your business and on the Group. Serious infringements have been seen to have a materially detrimental impact on the share price of infringing companies.

It is the responsibility of each business unit Managing Director (MD) within the Group to ensure that the business(es) for which they are responsible, and all relevant employees, understand and comply with the requirements of GDPR and this policy. Each MD must establish whether a Data Protection Officer should be appointed for the relevant business(es). For guidance, please contact your legal representative. The current Data Protection Officer for James Fisher and Sons plc is Danielle le Breton.

For further information regarding your rights as a data subject in relation to your own personal data, you should refer to the Employee Privacy Notice which is available on the Group Intranet.

Key Concepts

"Personal data" means any information relating to an identified or identifiable employee or other person (data subject). Personal data may be found in places such as databases, manual filing systems, word processing programmes, emails, CCTV records or internet logs.

"Processing" means anything that can be done with or in relation to data. It includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Special categories of personal data" means personal data revealing an employee's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Outline of the GDPR & Rights

Data Protection Principles

The GDPR stipulates that anyone processing personal data must comply with principles of good practice. These principles are legally enforceable.

These principles are as follows:

- **Lawfulness, fairness and transparency**: Personal data shall be processed lawfully, fairly and in a transparent manner. In particular, personal data shall not be processed unless specific conditions are met, and shall be processed in accordance with the rights of data subjects;
- **Purpose limitation**: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purposes or those purposes;
- **Data minimisation**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or the purposes for which it is processed;
- **Accuracy**: Personal data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose(s) for which it is processed, is erased or corrected or updated without delay;
- **Storage limitation**: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- **Integrity and confidentiality**: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, damage, using appropriate technical and organisational measures.

Lawfulness, Fairness and Transparency

You should not process any personal data unless the requirements for lawful and fair processing can be met. No personal data should be processed unless the processing is necessary:

- for the performance of the employment contract or other contract to which the data subject is a party, or in order to take steps at a data subject's request prior to entering into a contract; or
- for compliance with a legal obligation on the relevant Group company; or
- for the purposes of "legitimate interests" pursued by the relevant Group company or a third party.


Fisher

Processing of Special Categories of Personal Data

Additional safeguards exist for the processing of special categories of personal data (as defined above). You must not process data of this nature unless:

- you are informed by HR that the employee has freely given explicit consent to such processing;
- the processing is necessary in order to comply with any obligation or legal duty imposed on the relevant Group company, or to exercise specific rights of the employee in the field of employment law.
- the processing is necessary to protect the vital interests of the data subject or another person where they are incapable of giving consent (for example life threatening issues such as disclosure of a data subject's medical history to a hospital casualty department treating the data subject after a road accident).
- the processing is necessary for, or in connection with, legal proceedings (including prospective legal proceedings).
- the processing is necessary in the context of occupational health for the assessment of the employee's working capacity

Processing of Salary Information

On occasion HR receives requests from external organisations, such as mortgage lenders, requesting information about an employee's salary. Such information will only be given after obtaining the employees explicit consent.

Purpose Limitation

The purposes for which the Group will process personal data regarding employees are set out in the Employee Privacy Notice. You must familiarise yourself with the Employee Privacy Notice. It is your responsibility to ensure that you do not process personal data for purposes other than those set out in the Employee Privacy Notice.

Integrity and Confidentiality

Even if you do not handle personal data as part of your normal work, you have a responsibility to ensure that any personal data you see or hear is processed in accordance with this policy and goes no further. This might, for example, include information you overhear in a telephone conversation or are copied into in an email. In addition, any personal data relating to any people you manage or appraise must be kept by HR, rather than in your own files. N.B. e.g. CVs from job applications.

You must keep personal data secure. You must comply with security arrangements in place including information technology such as password-protected files and screen savers, other organisational arrangements including locks for drawers and filing cabinets and restricted access arrangements.

Never disclose personal data to other employees or a third party either orally or in writing until all appropriate checks have been made and you are satisfied that the disclosure amounts to fair and lawful processing in accordance with the principles set out in this policy. All unusual or potentially sensitive disclosures must be authorised by HR. Special categories of personal data must never be disclosed to third parties without the prior authorisation of HR who will verify the relevant individual's explicit consent. You should

protect against accidental disclosure such as, for example, someone near to you being able to read information over your shoulder.

Processing of criminal data is only permitted when authorised by law. If you become aware of any criminal data in respect of any individual, such information should not be recorded, disclosed or otherwise processed without the consent of HR.

James Fisher Principles on Handling Data

We are committed to compliance with the GDPR. In addition to compliance with all other obligations referred to in this policy the Group will apply the following principles:

- The Group will only gather and process as much information as is needed;
- The Group will identify the purpose in gathering information and decide when it is no longer required;
- The Group will consider whether the information gathered is sensitive and if so apply extra security measures;
- The Group will ensure the information held is accurate and will give employees the opportunity to correct any incorrect data;
- The Group will ensure all information is kept securely. All current employee information will be locked away in the human resources office;
- The Group will ensure that external contractors used to store past employee information guarantee safe storage; and
- The Group will delete or destroy and information which is no longer required.

Data Subject Rights

All subjects for whom personal information is being kept have rights which can be exercised under the GDPR.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information;
- The right to prevent processing in certain circumstances; and
- The right to correct, rectify, block or erase information regarded as wrong information.

Requesting Access to Personal Information

As set out in the Employee Privacy Notice, any employee may request access to their personal data held by the relevant Group Company. Any employees wishing to exercise this right should make their request in writing to the relevant human resources representative.

The relevant Group Company aims to comply with a request for access to personal information as quickly as possible, but must comply with a subject access request within one month of receipt of the request.

Individuals outside the direct employment of the Group such as contractors, customers and suppliers also have rights in relation to any personal data held by the Company, including a right of access.

If you receive a request in relation to rights under the GDPR, whether from an employee or a third party, this must be passed immediately to the relevant Data Protection Officer or the relevant Group HR representative.

Outsourcing of Data

In order for an organisation to perform a contract it may be necessary to supply them with items of personal data for employees, such as name, address, national insurance number and salary details.

Such data will be fairly and lawfully processed in accordance with Data Protection principles and it will also be ensured that data supplied will only be processed for the specific purpose of the contract.

The Company will ensure that contractors:

- Will only use and disclose the personal data in line with the Company instructions; and
- Take appropriate security measures to ensure information held is adequately protected.

Handling Sensitive Cardholder Information

If your business manages an e-commerce site as a sales route for your products or services, you must comply with the Group Credit Card Information Security Policy.

If your business directly handles and/or stores sensitive cardholder information for sales transactions for your products or services, you must implement a specific Information Security Policy.

Scope

This policy is for guidance only and does not form part of your contract of employment.

Approved by the Board of Directors of James Fisher and Sons plc on 2 May 2018