SMITH & SONS (BLETCHINGTON) LTD

DATA PROTECTION POLICY

INCLUDING LINEAR FISHERIES (OXFORD) LTD

Smiths Bletchington (the "Company") is committed to undertaking its business activities responsibly and sustainably, meeting the needs of customers, employees, and other stakeholders, while managing the social and environmental impacts of our activities.

Introduction

The Company and its subsidiaries need to gather and use certain information about individuals for a variety of business purposes.
This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data in manual and electronic records to which they have access in the course of their work. This policy requires staff to ensure that the Data Protection Responsible Person (DPRP) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

Scope

This policy applies to all locations of the Company.
It also applies to all job applicants, existing and former employees, apprentices, volunteers, contractors, suppliers, and other people working on our behalf. This policy supplements our other policies relating to internet and email use. This policy ensures that we comply with data protection law and follow good practice. It protects the rights of staff, customers, and partners. It ensures that we are open about how we store and process individuals' data and protects us from a data breach. It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 2018.
The business purposes for which personal data could be used include:

- Compliance with our legal, regulatory, and corporate governance obligations and good practice.
- Gathering information as part of investigation by regulatory bodies or in connection with legal proceedings or requests.
- Ensuring business policies are adhered to (such as policies covering email and internet use).
- Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking.
- Investigating complaints.
- Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and facilities and staff absences, administration, and assessments.
- Monitoring staff conduct, disciplinary matters.
- Marketing our business.
- Improving services.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.
Personal data we may gather includes but not limited to:

- Individuals contact details including email addresses for individual and next of kin.
- Education, skills, details of qualifications
- Financial and pay details including tax codes.

- Marital status.
- Nationality.
- Job title, job descriptions and pay grades.
- Terms and conditions of employment
- Curriculum vitae and other information gathered during recruitment.
- References from former employers
- National insurance numbers
- Conduct issues such as letters of concern, disciplinary proceedings
- Holiday records
- Internal performance information
- Medical or health information
- Sickness absence records
- CCTV images.
- IP address for website users.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.
Any use of sensitive personal data should be strictly controlled in accordance with this policy.

Data Protection Law

The General Data Protection Regulation (GDPR) describes how organisations, including the Company, must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. It must be accurate and kept up to date and not held any longer than necessary. It must be processed in accordance with the rights of data subjects and not transferred outside the European Economic Area Economic Area (EEA) unless that country or territory also ensures an adequate level of protection level of protection.

Responsibilities
The Board of Directors is ultimately responsible for ensuring that the Company meets its legal obligations.
Under GDPR the company is deemed a Data Controller.

The Data Protection Responsible Person is responsible for:

- Keeping the board updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the company holds on the term (subject access requests).
- Checking and approving any contracts or agreements with third parties that may handle the company's special data.
- Ensuring compliance with the Data Protection Code of Practice for Surveillance Cameras and Personal Information where applicable.

The IT Manager is responsible for:

- Ensuring all systems, services, and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The Commercial and Distribution Manager is responsible for:

- Approving any data protection statements attached to communications such as email and letters.
- Addressing any data protection queries from clients, target audiences and media outlets.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.

Procedures:

General guidelines:

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The Company will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure by taking sensible precautions and following the guidelines held within Company policies.
- Strong passwords must be used and never shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Reporting Breaches:

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Information Commissioner within 72 hours of any compliance failures that are material either in their own right or a part of a pattern of failures.

Subject Access Requests

All individuals who are the subject of personal data held by the company are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

Any subject access requests from individuals should be made by email, addressed to the Data Protection Responsible Person at info@smithsbletchington.co.uk
The Data Protection Responsible Person will aim to provide the data within one calendar month.
The Data Protection Responsible Person will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without consent of the data subject.
Under these circumstances, the Company will disclose requested data. However, the data protection responsible person will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

The Company aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the company's websites.