



## **DATA PROTECTION POLICY**

It is a legal requirement for the Company to comply with the Data Protection Act, 1998. It is also Company policy to ensure that every employee maintains the confidentiality of any personal data held by the Company in whatever form.

### **Data protection principles**

The Company needs to keep certain information about its employees, customers, and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This means that we must comply with the Data Protection Principles set out in the Data Protection Act, 1998.

These principles require that personal data must be:

- Obtained fairly and lawfully and shall not be processed unless certain conditions are met.
- Obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose.
- Adequate, relevant and not excessive.
- Accurate and up-to-date.
- Kept for no longer than necessary.
- Processed in accordance with data subjects' rights.
- Protected by appropriate security.
- Not transferred to a country outside the European Economic Area without adequate protection.

In processing or using any personal information you must ensure that you follow these principles at all times.

### **Data protection co-ordinator**

To ensure the implementation of this policy the Company has designated the Managing Director as the Company's Data Protection Co-ordinator. All enquiries relating to the holding of personal data should be referred to her in the first instance.



## **Notification of data held**

You are entitled to know:

- What personal information the Company holds about you and the purpose for which it is used.
- How to gain access to it.
- How it is kept up-to-date.
- What the Company is doing to comply with its obligations under the 1998 Act.

This information is available from Gary Hepburn.

## **Individual responsibility**

As an employee you are responsible for:

- Checking that any information that you provide in connection with your employment is accurate and up-to-date.
- Notifying the Company of any changes to information you have provided, for example changes of address.
- Ensuring that you are familiar with and follow the Data Protection Policy.

Any breach of the Data Protection Policy, either deliberate or through negligence may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

## **Data security**

You are responsible for ensuring that:

- Any personal data which you hold, whether in electronic or paper format, is kept securely.
- Personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.
- Items which are marked 'Personal' or 'Private and Confidential', or which appear to be of a personal nature, are opened by the addressee only.

You should not use your office address for matters that are not work-related.