

IMS Policy 04	Issue 01 Rev 02	DATA PROTECTION AND HANDLING POLICY	
Quality ISO 9001: 2015			
Environmental ISO 14001: 2015			
Health & Safety ISO 45001: 2018			

Use of Company Data & Protection of Personal Data

Use of Data by Employees

All data referring to suppliers, customers and employees must not be disclosed to unauthorised persons or used for unauthorised purposes. Breaches of this policy may result in disciplinary action.

Any supplier, customer and employee data that qualifies as Personally Identifiable Information (PII) is also subject to the Data Protection Act and should be handled accordingly. Note that there are significant personal and corporate penalties for misuse of PII.

Any employee or authorised third-party using a computer must comply with the company policy. This includes employees using company computer equipment in their own home or accessing data via their own devices.

Personal Data

The Company holds two kinds of personal data about you. Formal employee data and informal employee data.

The following are examples of formal employee data which the Company is likely to hold on computer or in manual files: CVs; application forms; test results; interview notes; contracts of employment; medical notes and records; appraisal records; accident records; performance ratings; training notes; attendance records; payroll records; disciplinary action or grievance notes; redundancy or redeployment records; pension, pay and benefits; sales/commission; financial reference; equal opportunities-monitoring information; company car documentation; medical certificates; time sheets; employer references; next of kin/emergency contacts; relevant criminal convictions/proceedings (if any exist); images of staff where appropriate (e.g. ID cards, photos, CCTV footage).

The following are examples of informal employee data.

This data is often of a transitory nature and includes the information retained by managers for day-to-day management purposes: detailed working rotas; notes relating to employees' training needs; notes recording team roles; notes detailing short-term resource issues; notes and records of day-to-day matters.

The information described above will be available only to HR department. It will only otherwise be disclosed as relevant and appropriate for the purposes described below, or where strictly necessary (for example in a disciplinary process, employee development or in cases of emergency).

The Company recognises that certain types of data, including some of the categories above, are particularly sensitive. This includes, for example, information in relation to such matters as racial or ethnic origin, and physical or mental health or condition. The Company may use sensitive information to help it comply with its legal obligations for example the company may use information about your racial/ethnic origin for its equal opportunities monitoring and information about your physical/mental health or condition to meet its obligations under the Disability Discrimination Act 1998, Equality Act 2010 and others. Although inevitably there will be a need for the Company to process sensitive data on occasions, the Company will seek to keep such processing to a necessary minimum.

The information will typically be used for: personnel and payroll administration; work management; business analysis; employee monitoring (e.g. for compliance with the Company's policies and procedures); legal compliance.

IMS Policy 04	Issue 01 Rev 02	DATA PROTECTION AND HANDLING POLICY	 WORKING FOR THE FUTURE
Quality ISO 9001: 2015			
Environmental ISO 14001: 2015			
Health & Safety ISO 45001: 2018			

Employee Monitoring

Employees should be aware that in order to ensure compliance with its legal obligations and its internal policies and procedures (including in particular its Diversity, Harassment, and E-mail, Fax and Internet Policy); the Company may monitor employee communications and other activities in the following ways:

E-mail facilities and Internet access are provided to employees for business purposes and, therefore, the Company reserves the right to review e-mail messages. Nothing should be written in email that would be suitable in a letter or memorandum. Electronic messages are admissible as evidence in libel proceedings and have been used successfully in libel cases. Matters of a personal or sensitive nature should not be transmitted by email unless absolutely unavoidable and thought should always be given to alternative methods of communication.

In some circumstances, the Company tapes incoming and outgoing telephone calls for training and other purposes.

The Company may employ CCTV cameras in various reception, business, operational and staff areas. Cameras are also fixed to vehicles. These cameras are installed for the purposes of crime prevention and public and employee safety. Information gathered may be used for disciplinary purposes if found necessary,

Please refer to the Company's policies on Diversity, Bullying and Harassment and E-mail, Fax and Internet Policy, which can be found within this Employee Handbook.

The Company will monitor employees only where, and in a manner that it considers proportionate to the problem it is seeking to address in carrying out the monitoring. Relevant employee rights, including privacy rights will be taken into account in deciding this.

Signed:



..... Date: ...1st March 2023.....

Managing Director
David Hughes