Data Protection Policy

Diving Survey and Marine Contracting Limited (DSMC) is committed to processing data in accordance with our responsibilities under the General Data Protection Regulations (GDPR). The company will monitor its storage and information processes at frequent intervals in accordance with current legislation and to ensure its continued compliance within the remit of its Data Protection Registration. Any information that is found to be materially incorrect will be amended as soon as is practical or destroyed.

Personal Data

Personal Data is data consisting of information which relates to a living individual who can be identified from the information. Personal data includes expressions of opinion about an individual. All personal data must be processed in accordance with the Data Protection Act 2018, a UK Act of Parliament which compliments the European Unions GDPR regulations. The company will ensure that its employees are aware of their requirement to treat personal data appropriately and, where applicable, will treat breaches of its requirements under the Data Protection Act seriously, which may include disciplinary action.

In addition, and under the Data Protection Act, the company and others acting on its behalf, will collect, retain and process information about its employees. The type of information which may be obtained and stored by the company includes (but is not limited to) dates of birth, sex, health and the commission or alleged commission of any offences. This information will be used for payroll and personnel management purposes in connection with each individuals employment with the company. In addition, the company shall use any data it holds to ensure it can monitor and comply with any current legislation, particularly in terms of equal opportunities and non-discrimination. Where the company holds any employee's personal data, it shall check this data from time to time to ensure that it remains accurate. This shall be carried out on a regular basis by contacting each employee to confirm the details held on file. Employees who become aware of a material change to their circumstances, such as their personal details/maiden names/aliases, home address, next of kin or any contact phone numbers, is required to notify the company as soon as is practical.

The company may also collect and store data on any other persons associated with the carrying out of its business, or as part of its recruitment and/or training programme. Wherever possible, any information stored will be verified as correct and accurate.

Data Security, Confidentiality and Privacy

All data or information sorted or processed on the organisation's systems or transmitted within or from the organisation (e.g. e-mail, voice-mail) is the property of the organisation and may be accessed, read or monitored accordingly. Any employee with access to company IT resources must ensure the confidentiality and appropriate use of any accessible data, by being aware of the company cyber security policy and the ongoing need to abide by the policy.

All employees are required to abide by the privacy rights of all other employees regarding the disclosure of personal information, as required by current legislation. It should also be noted that disclosure of confidential information to unauthorised persons or entities, or the use of such information for self-interest or advantage, is prohibited, as is access to non-public areas of any network drive. Breaches will be treated severely under the company disciplinary rules.

Privacy

All users of the company's IT resources are advised to consider the open nature of information disseminated electronically and should not assume any degree of privacy or restricted access to such information. The company strives to provide the highest degree of security when transferring data but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed, or misused by others.

Though it is not the intention of the company to continuously monitor Internet and e-mail communications, or access data files held by an individual, the company reserves the right to do so at any time. The company has the right to read and/or delete any data stored on company owned or leased equipment. All employees must be aware that they therefore have no right of privacy in respect to Internet and e-mail communications, or stored data, utilising company owned or leased equipment.

However, it should be noted that the company would not normally access an employee's data or communications without first requesting permission to do so. However, in the event of an internal disciplinary investigation, or at the request of a Government Agency, or as a result of litigation against the individual and/or company, any e-mail or data files may be locked and/or copied to prevent destruction and loss of information. In such cases, the company may resort to its right to view any data held without first requesting the permission of the individual concerned.

DMSC takes data security seriously in accordance with its Cyber Security Policy, in the event unlikely of a data breach DSMC will endeavour to contact all persons affected so they can take appropriate security measures.

Although DSMC's data protection procedures are not currently accredited to any external third party standard, it is my aim to have these procedures audited and accredited as being compliant with the ISO 27001 standard by the end of 2026.

Charlie Bayston
Managing Director
4th December 2024