

# Confidentiality Statement

September 2014



**Confidentiality Statement**

Issue 4, September 2014

**Confidentiality Statement**

This Confidentiality Statement is intended to apply to all employees, agency staff, contractors and consultants working for or with any VolkerWessels UK company who, as a result of that work, become aware of any confidential information regarding the Company's commercial and business activities or information regarding any client's suppliers ('**Confidential Information**').

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat information in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, and others that we communicate with. Personal data may also include data pertaining to our clients, our stakeholders and our supply chain. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

This Confidentiality Statement does not supersede other documentation where this subject is mentioned and should be read in conjunction with the ICT Policy, Employee Handbook and Statement of Main Terms and Conditions.

By signing that you agree with this Statement, you agree that you will at all times, whether you are employed or engaged by or otherwise contract with VolkerWessels UK or any of its employing entities (hereafter referred to as 'the Company') and except where such information is in the public domain.

Maintain the strictest secrecy with regard to the business affairs of the Company, any other VolkerWessels UK Group companies and their customers, except to the extent that you may be authorised to disclose them by the Board of Directors of the Company, a Court of Law or any authorised or enforcement agency such as the Police, a Regulatory Body given powers under the Financial Services Act, HM Revenue & Customs, etc. You understand that any breach of this agreement could result in the Company's sensitive and confidential data being disclosed to competitive or other interested parties.

Any breach of this statement will be taken seriously and may result in disciplinary action, and may in appropriate circumstances be considered to amount to gross misconduct.

Any questions or concerns about the operation of this statement should be referred in the first instance to the Head of HR or Chief Finance Officer.

**Protecting the business**

During the course of your employment, you may acquire significant knowledge of the Company's business and have access to business contacts. The Company's business may be damaged if you disclose information relating to its technology, strategic plans, finances or client connections to another party.

**Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

**Personal data** means data relating to an individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as name, bank account details, address or date of birth) or it can be an opinion (such as a performance appraisal). Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership,

**Confidentiality Statement**

Issue 4, September 2014

**Confidentiality Statement (Continued)****Protecting the business (Continued)**

medical data including physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

**Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

All personal and sensitive personal data must be kept strictly confidential and not be directly or indirectly revealed, reported, copied, published, communicated, disclosed or made available to any third party. Permission must not be given to others to use confidential information, other than for legitimate business purposes and with appropriate authorisation.

**Data security**

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Access to personal data may only be given to any employee or relevant third-party data processor if that person agrees to comply with this statement. Only people who are authorised to use the data can access it.

When sharing or transmitting personal or sensitive data internally or externally to a third party, this data should be anonymised where possible.

Where personal or sensitive data has been requested that includes names or other information meaning that individuals can be easily identified, please seek advice from your HR Representative before disclosing.

**Confidentiality Statement**

Issue 4, September 2014

**Confidentiality Statement (Continued)****Security procedures include:**

- **Secure lockable desks and cupboards** - desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- **Methods of disposal** - paper documents should be securely shredded. Please refer to the ICT Department regarding disposing of electronic information.
- **Equipment** - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock their PC when it is left unattended.
- **Removal of data** - confidential and sensitive information should not be removed from the workplace without prior consent from the Company.
- **Transfer of Data** - confidential and sensitive information should not be transferred either in paper or electronic format, without prior consent from the Head of HR or Chief Finance Officer. Where information is transferred electronically, the information should be contained within a document that is password protected and the password should not be sent in the same email as the document.

**Providing information over the telephone**

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

**Providing information by fax machine**

- Sensitive and confidential information should only be transmitted by fax machine in exceptional circumstances and should be restricted to the minimum information necessary.
- Only use names and addresses when absolutely necessary and anonymise information where possible.
- Always use a cover sheet with a confidentiality statement.
- Contact the recipient to inform them that a confidential fax is being sent and ask them (or someone on their behalf) to wait at the receiving end.
- Obtain confirmation of receipt from the intended recipient of the fax.

**Leaving the company**

Any person provided with access to personal data shall hand back to the Company any confidential information and all copies thereof (in whatever media) in their possession and will remove / destroy all confidential information contained within computers, storage equipment (i.e. cd's, memory sticks) or other electronic devices that are not returned to / retained by the Company.

**Confidentiality Statement**

Issue 4, September 2014

**Confidentiality Statement (Continued)**

The return of confidential information shall not release individuals from their obligations under this Confidentiality Statement.

---

I have read and understood the Confidentiality Statement and agree to abide by the terms and conditions.

Signed: \_\_\_\_\_

Clearly Print Name : \_\_\_\_\_

Date: \_\_\_\_\_