3.18 **DATA PROTECTION**

Everyone has rights with regard to how their personal information is handled. During the course of the company's activities it will collect, store and process personal information about its staff, and the company recognises the need to treat it in an appropriate and lawful manner.

The types of information that the company may be required to handle include details of current, past and prospective employees, suppliers, customers and others that the company communicates with. 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 the company may use that information.

Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy sets out the company's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

Any questions or concerns about the operation of this policy should be referred in the first instance to your department manager.

If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the HR manager.

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

Data subjects for the purpose of this policy include all living individuals about whom the company holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in the company's possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The company is data controller of all personal data used in its business.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the company's data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

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.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, 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. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

3.18.1 **Data Protection Principles**

Anyone processing personal data must comply with the eight principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

3.18.2 **Fair and Lawful Processing**

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the O&M company employing you) and the purpose for which the data is to be processed by the company, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that you have consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases your explicit consent to the processing of such data will be required.

3.18.3 **Processing for Limited Purposes**

Your personal data may only be processed for the specific purposes notified to you when the data is first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which your data is processed, you will be informed of the new purpose before any processing occurs.

3.18.4 **Adequate, Relevant and Non-excessive Processing**

Your personal data will only be collected to the extent that it is required for the specific purpose notified to you. Any data which is not necessary for that purpose will not be collected.

3.18.5 **Accurate Data**

Your personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

3.18.6 **Timely Processing**

Your personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from the company's systems when it is no longer required.

3.18.7 **Processing in Line with Data Subject's Rights**

Your data must be processed in line with your rights as a data subject. Data subjects have a right to:

- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended;
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

3.18.8 **Data Security**

The company will 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.

The Act requires the company to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Your personal data may only be transferred to a third-party data processor if that third party agrees to comply with those procedures and policies, or if that third party puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it;
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed;
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data will therefore be stored on the company's central computer system instead of individual PCs.

Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported;
- **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 shredded. Floppy disks and CDROMs should be physically destroyed when they are no longer required;
- **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

3.18.9 **Dealing with Subject Access Requests**

If you wish to make a formal request for information that the company holds about you, you must do so in writing. A fee is payable by the data subject for provision of this information. If you receive a written request, you should forward it to the HR manager immediately.

3.18.10 **Providing Information Over The Telephone**

If you are dealing with telephone enquiries, you should be careful about disclosing any personal information held by the company. In particular you 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 you are not sure about the caller's identity and where their identity cannot be checked;
- Refer to your line manager or department manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

3.20 **INTERNET AND E-MAIL**

3.20.1 **Introduction**

This policy establishes guidelines for the use and security of the company's communication networks, which include e-mail, Internet, telephone, fax and voicemail systems whether used on the company's premises or elsewhere. This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff. Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

This policy should be read in conjunction with any other instructions and rules issued by the company from time to time including, but not limited to, the Social Media Policy.

3.20.2 **General Policy**

This policy, and all associated documents, applies to the use of the company's computer network, computers (whether fixed or portable) and any other computing, data processing or telecommunications device (including any iPhone or similar portable equipment) provided by or made available to you by the company or used in the company's premises (**the IT System**) and any use by you of the company's Internet and e-mail facilities.

The objectives of this policy are to ensure that:

- You use the IT System and the company's Internet and e-mail facilities in a professional and responsible manner.
- Any legal requirements regulating the IT System are complied with.
- The integrity, performance and security of the IT System are maintained.
- There is no use of the IT System which:
  - Is illegal and/or breaches the terms of this policy; or
  - Interferes with your or another employee's performance; or
  - Reduces the performance of the IT System; or
  - Damages or could damage the reputation of the company.

Computer systems and networks, the Internet and e-mail play an increasingly active part in the company's business. The use of such systems and networks provides the potential for access to inappropriate information and illegal activities, for the IT System to be attacked by viruses and other forms of malicious software and for hackers to access and disrupt the IT System.

The company is therefore entitled to protect itself and its employees and it is important that the terms of this policy are complied with at all times. Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the company's equipment or facilities are used for the purpose of committing the breach. Anyone subject to any investigation in respect of any alleged breach of this policy will be required to co-operate with that investigation, which may involve providing details of all relevant passwords and logins. Individuals may also be required to remove Internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

3.20.3 **Electronic Communications**

Electronic communication can be carried out through a wide range of technologies including, but not limited to:

- The use of the IT System.
- E-mail sent using any of the company's IT resources.
- Internet usage involving any of the company's IT resources.
- Instant messaging services broadcast in any method or means involving any of the company's IT resources.

- The use of the company's telecommunications systems (including fax, voicemail and text messaging).
- The physical exchange of media, for example, the use of memory sticks or other electronic storage devices.
- Wireless exchanges, for example, Bluetooth or infra-red.

3.20.4 **Monitoring of Electronic Communications**

The contents of the company's IT resources and communications systems are its property. Therefore, you should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on the company's electronic information and communications systems. Do not use the company's IT resources and communications systems for any matter that you wish to be kept private or confidential from the company.

The company reserves the right to monitor, intercept and review, without further notice, all activities using the company's IT resources and communications systems, including, but not limited, to social media postings and activities, to ensure that all relevant rules are being complied with and that all activities are for legitimate business purposes. You consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The company may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

3.20.5 **Permitted Use of Electronic Communications**

The IT System and Internet and e-mail facilities are provided for the conduct of the company's business. Incidental and limited personal use of these systems is permitted, provided it does not interfere with the proper performance of your role or conflict with any business activity. You should consider whether it is appropriate to give your business telephone number and e-mail address to those who will not be using it for business purposes.

Limited personal use of the IT System and Internet and e-mail facilities is always at the discretion of IT Manager and such permission may be withdrawn if you are considered to be abusing this permission or for any other reason. Excessive, unreasonable or inappropriate use of the company's time, IT System and Internet and e-mail facilities for personal matters, whether during or after normal office hours, is prohibited and will be regarded as a disciplinary issue and in serious cases could lead to dismissal.

E-mail correspondence is no different from hard copy letters, memoranda and reports and can be used in legal proceedings. Even where you have deleted a message from individual computer records, these may still be held on the company's or a third party's file servers or as part of routine data back-up. Under certain circumstances, Courts of Law can order the company to produce both internal and external e-mail records as evidence in Court in cases involving clients or others in litigation with the company. Please be aware that internal and external e-mail communications feature increasingly in Court cases and regulatory actions, with substantial damages being awarded for defamation and other conduct where the offending statements were sent by e-mail.

3.20.6 **Prohibited Use of Electronic Communications**

You must not transmit electronic communications which contain:

- Personal references. This does not include professional references issued by department managers and/or directors using the pre-agreed template.
- Price sensitive information relating to a public company.
- Confidential information relating to the company or its business or relating to any of its employees, contractors, suppliers, clients, customers or contacts.

- Formal notices.
- Defamatory statements.

You must not use electronic communications in any way which would potentially harm or damage the company's reputation or its relationship with clients or suppliers. This includes potentially defamatory messages, which criticise individuals or organisations.

Access to certain sites may only be permitted during fixed hours in order to allow staff access to normally restricted sites outside of their normal working hours, this does not affect the application of this or any other policies.

You must not use the company's IT System or Internet or e-mail facilities to view, access, download, save, receive, forward or send material related to or including:

- Offensive content of any kind, including pornographic material.
- The promotion of discrimination on any grounds.
- Threatening, bullying or harassing messages.
- Illegal activities.
- The operation of a personal business or the soliciting of money for personal gain.
- Originating or distributing e-mail chain letters.
- Sending unsolicited or spam e-mails.
- Viruses, malicious software or Trojan horse programmes.
- Wrongfully obtaining material protected under copyright laws.
- Misrepresenting the communication sender's identity.
- Attempting to gain unauthorised access to any computer system of the company or any other organisation.

If you consider that any communication, whether an e-mail, voicemail, fax or other electronic communication, received falls within the above categories, you should not respond to it and must report it immediately to the IT Manager

You must not forward work, e-mails or other business-related communications from the company's IT System to or from a personal e-mail address or computer (whether or not such e-mails contain confidential information) and access to personal e-mail accounts on the company's IT System is strictly forbidden, save with the prior written approval of the IT Manager. For the avoidance of doubt, this handbook, your personal contract of employment, your own payslips and other payroll information relating to you can be forwarded to your personal email address.

You should note that the above prohibitions apply equally to business and personal communications.

3.20.7 **Compliance with Legal Requirements**

You must comply with all software licences, copyrights and all laws governing intellectual property and on-line activity.

3.20.8 **Safeguarding the IT System and Electronic Data**

Information about the company and its clients is highly valuable and must be protected and safeguarded. You should take care to ensure that the company's information held on the IT System or any other device is not lost, disclosed, modified without authorisation or accessed by third parties. This means:

- Any modifications to the IT System, including modifications to or additions of hardware or software, must be approved by the company. You must not download any software from the IT System or load any software onto the IT System whether from the Internet or otherwise without prior written / email authorisation from the IT Manager.
- You must not disable or modify IT security features provided by the company including the use of anti-virus software, access controls, hard disk encryption software and firewalls.

You have a responsibility to maintain good housekeeping practices on all electronic data. This should include, but is not restricted to, the timely review and filing of e-mails and the removal of surplus or

additional copies of sensitive data from the IT System, e-mail accounts and electronic storage devices.

You must exercise due care to ensure that the company's IT equipment is protected from damage, loss and theft, in particular:

- Laptops must be secured whenever and wherever they are in use and should be kept in a lockable cupboard overnight or if left for a prolonged period of time.
- Care should be taken when moving equipment, as it contains sensitive components. Suitable carrying cases should be used.
- Unless locked away and out of sight, laptops should never be left unattended in a car or any location accessible by the public.
- No one other than an authorised employee or contractor of the company should use or have access to the company's IT System. Employees given laptops and other IT equipment should keep them out of reach of children and persons who are not employees of or engaged by the company.

In the event of damage to, theft or loss of any of the company's IT equipment, you should immediately notify your line manager and/or the IT Manager. As soon as is reasonably practicable, you must provide your line manager with all relevant details of the theft/loss and make a report to the police.

Access to any IT system or electronic data held on behalf of the company must be password protected. Passwords are the principal means of identifying a user and, in the interests of data security, they must be carefully controlled. It is your responsibility to ensure that your password is robust, protected and kept confidential.