IT POLICY

Rev 1

Issued April 2024

Managing Director - Kevin Hague

AARSLEFF CENTRUM CANNON PILING a part of Aarsleff Ground Engineering Limited

1. POLICY STATEMENT

1.1 This policy applies to all companies within Aarsleff Ground Engineering Ltd UK and Avoncross Ltd, including companies trading as Centrum Pile and Cannon Piling (referred to in this statement as 'The Company').

1.2 This policy is non-contractual, and the Company reserves the right to amend or withdraw the policy at any time at the Company`s discretion.

1.3 The Company expects their employees to demonstrate honesty, integrity, and fairness in all aspects of their duties carried out on behalf of the Company.

1.4 Similarly, relationships with all stakeholders including clients and suppliers will be at all times conducted professionally and to high ethical standards.

1.5 The contents of this policy and all revisions which may be made will be brought to the notice of all employees.

1.6 The Company will operate a 'zero tolerance' approach to any breach of this policy. Any such breach will be treated as gross misconduct.

1.7 This policy will form part of the Integrated Management System and be formally reviewed annually by Senior Management.

2. ABOUT THIS POLICY

2.1 The purpose of the IT policy is to provide a framework to ensure that there is continuity of procedures in the usage of computer systems, equipment, internet, and e-mail within the Company.

2.2 To ensure that we can utilise the system to its optimum we have devised a policy that provides maximum use of the facilities whilst ensuring compliance with the legislation throughout.

2.3 The IT Policy sets out acceptable and unacceptable use of Company IT systems, internet, email, and mobile device equipment.

2.4 This Policy applies to all Company employees. You must read, understand, and comply with policy when processing personal data on our behalf and attend training on its requirements. This policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

3. ROLES AND RESPONSIBILITES

3.1 The Board of Directors have overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

3.2 Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it.

3.3 This Policy applies to all Company employees, Agency and Sub-contractors. You must read, understand, and comply with policy when using Company systems and attend training when required.

3.4 This policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

4. VIRUS PROTECTION PROCEDURES

4.1 To prevent the introduction of virus contamination into the software system the following must be observed:

4.2 Unauthorised software including public domain software, USBs, external hard drives, CDs or internet downloads must not be used.

4.3 All software must be virus checked using standard testing procedures before being used. Please contact the IT Manager or raise a ticket through the (virus checked by IT)

5. USE OF COMPUTER EQUIPMENT

5.1 To control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

5.1.1 The introduction of new software must first of all be checked and authorised by the IT Manager before general use will be permitted.

5.1.2 The Company uses *Microsoft Intune*, this enables the management and control of all internal apps, platforms, data, and resources. It gives the ability to report on any unauthorised software and is used on all Company PC's and mobile devices.

5.1.3 Only authorised employees should have access to the Company's computer equipment.

5.1.4 Only authorised software may be used on any of the Company's computer equipment.

5.1.5 No software may be brought onto or taken from the Company's premises without prior authorisation.

5.1.6 Unauthorised access to the computer facility may result in disciplinary action.

5.1.7 Unauthorised copying and/or removal of computer equipment/software may result in disciplinary action, such actions could lead to dismissal from the Company.

6. E-MAIL AND INTERNET USE

6.1 Where appropriate, duly authorised employees are encouraged to make use of the Internet as part of their official and professional activities.

6.2 Where personal views are expressed, a disclaimer stating that this is the case should be clearly added to all correspondence.

6.3 The intellectual property right and copyright must not be compromised when publishing on the Internet. Any employee who seeks to publish information on the internet must gain guidance and approval from the Marketing Team

6.4 The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material or material that is not work-related during working hours, leaves an individual liable to disciplinary action which could lead to dismissal.

6.5 PROCEDURES – ACCEPTABLE/ UNACCEPTABLE USE

6.5.1 Unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.

6.5.2 The internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:

6.5.2.1 Comply with all our internet standards.

6.5.2.2 Access during working hours should be for business use only.

6.5.2.3 Private use of the internet should be used outside of your normal working hours.

6.5.3 The Company will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:

6.5.3.1 Accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights.

6.5.3.2 Non-compliance of our Social Media Policy.

6.5.3.3 Connecting, sending, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material.

6.5.3.4 Engaging in computer hacking and other related activities or attempting to disable or compromise security of information contained on the Company's computers.

You are reminded that such activities (6.5.3.3 and 6.5.3.4) may constitute a criminal offence.

6.5.4 Email used correctly is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims.

6.5.5 Unauthorised or inappropriate use of the email system may result in disciplinary action which could include summary dismissal.

6.5.6 The email system is available for communication and matters directly concerned with the legitimate business of the Company. Employees using the email system should give particular attention to the following points:

6.5.6.1 All comply with Company communication standards.

6.5.6.2 Email messages and copies should only be sent to those for whom they are particularly relevant.

6.5.6.3 E-mail should not be used as a substitute for face-to-face communication or virtual contact. Abusive emails must not be sent. Hasty messages sent without proper consideration can cause upset, concern, or misunderstanding.

6.5.6.4 If an email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Company will be liable for infringing copyright or any defamatory information that is circulated either within the Company or to external users of the system; and all colleagues should take care not to share personal/ colleague information that would infringe on the General Data Protection policy, for example the sharing of personal email addresses.

6.5.6.5 Offers or contracts transmitted by email are as legally binding on the Company as those sent on paper.

6.5.7 The Company will not tolerate the use of the e-mail system for unofficial or inappropriate purposes, including:

6.5.7.1 Any messages that could constitute bullying, harassment or other detriment;

6.5.7.2 All employees should be mindful of their personal use of email and the internet (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters) any unacceptable use may be deemed a disciplinary matter and would follow the normal disciplinary procedures.

6.5.7.3 on-line gambling.

6.5.7.4 accessing or transmitting pornography.

6.5.7.5 Any unauthorised transmitting of copyright/ confidential information and/or any unauthorised software available to the user; or

6.5.7.6 Posting confidential information about other employees, the Company or its clients or suppliers. Any unacceptable use may be deemed a disciplinary matter and would follow the normal disciplinary procedures.

6.6 Monitoring

6.6.1 We reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements.

6.6.2 This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account.

6.6.3 Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring your usage will mean processing your personal data.

6.6.4 You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the GDPR Policy

6.7 USE OF SOCIAL NETWORKING SITES

6.7.1 Any work-related issue or material that could identify an individual who is a client or work colleague, which could adversely affect the Company, a client or our relationship with any client must not be placed on a social networking site. Please also refer to the Social Media Policy.

6.7.2 This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment or mobile device. For further guidance please read our Social Media policy and Disciplinary Policy.

7 IT EQUIPMENT AND COMPANY MOBILE DEVICES

7.1 All IT equipment including Company mobile devices should be treated with care, they are expensive pieces of Company equipment. If damaged, lost or stolen this should be reported immediately.

7.2 If a PIECE OF Company IT equipment or Company mobile device is lost, stolen or damaged the Company will charge the user for the cost of a replacement.

7.3 For the first replacement the charge will be at 50% of the cost of replacement, any further replacement will be charged to the employee via payroll at 100% of the replacement cost.

7.4 The Company devices are to be used for business purposes only except in the case of an emergency. Device calls in work time, personal calls or excessive data use may be investigated as part of the Disciplinary procedure and;

7.5 Any personal use deemed excessive by the Company may be repayable by the employee. The Company reserve the right to deduct the appropriate sums from your salary in the event that repayments are not made.

7.6 Internet usage on Company devices is subject to the same provisions set out in our Email and Internet Policy. The Company reserves the right to monitor all communications made on Company devices in order to ensure compliance with our policies and procedures.

7.7 All equipment must be treated with due care and attention. Faulty, lost or stolen equipment should be reported to the IT Manager/ IT Team as soon as possible, tickets can be raised via the IT Helpdesk system via Jira Service Management system: IT Support - Jira Service Management (atlassian.net)