Pendragon | PLC

Adopted : 17 December 2019

INFORMATION TECHNOLOGY & COMMUNICATIONS SYSTEMS ACCEPTABLE USE POLICY 2019 - 2020

Pendragon PLC, together with its affiliates and subsidiary companies (together, “Pendragon”, the “Company”, “we”, “us” or “our”) provide computers, networks, communication systems and other IT resources for use for business purposes only during working time and at all other times. To protect the Company and its employees, it is the Company’s policy to restrict the use of all IT resources and communications systems as described below. Each user is responsible for using our systems and resources.

The use of the Company’s IT resources and communication systems by a team member, whether on a temporary or permanent basis, shall signify his or her understanding of and agreement to the terms of this policy, as a condition of employment. In addition, we expect all who use our IT resources and communication systems, including agency workers, contractors and sub-contractors or other third parties (“third party users”) to act in accordance with, and at all times adhere to this policy when doing so.

The Legal Department, in conjunction with the Human Resources Department and Pinewood Technologies PLC is responsible for the administration of this policy.

DEFINITIONS USED IN THIS POLICY

Pendragon Group means Pendragon PLC and any company over which Pendragon PLC has exercised or is entitled to acquire direct or indirect control over that company’s affairs, control to have the same meaning as in section 450 of the Corporation Taxes Act 2010.

ACCEPTABLE USE PRINCIPLE

We recognise that the confidentiality, integrity and availability of information, in all its forms, is crucial to the ongoing success of our business and its good governance. Failure to adequately secure and protect information increases the risk of financial and reputational losses. This policy should be considered in particular, in conjunction with The Company’s Data Protection & Privacy, Information and Cyber Security Policy, the Social Networking Sites Policy, and the Diversity and Equal Opportunities Policy, all of which apply to the use of the Company’s IT resources and communication systems by its team members and, where relevant, third party users.

Team members and third party users are expected, at all times, to use and operate our computers, networks, communication systems and other IT resources:-

(a) at all times in a productive, ethical and lawful manner;

(b) with integrity and honesty;

(c) for the business purpose for which they have been provided;

(d) in a manner which cannot be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by law.

SECURITY, ACCESS AND PASSWORDS

Security of our IT resources and communications systems is the responsibility of Pinewood Technologies PLC, including approval and control of team members' and others access to systems and suspension or termination of access in the cases of misuse or when a user is no longer a team member or otherwise ineligible to use the systems.

It is the responsibility of each team member to adhere to any IT security guidelines issued by Pinewood Technologies PLC from time to time, including but not limited to the creation, format and scheduled changes of passwords. All user names, pass codes, passwords and information used or stored on the company's computers, networks and systems are the property of the Pendragon Group. No team member may use a user name, pass code, password or method of encryption that has not been issued to that team member or authorised in advance by the Company.

No team member shall share user names, pass codes or passwords with any other person. A team member shall immediately inform Pinewood Technologies PLC if he knows or suspects that any user name, pass code or password has been improperly shared or used, or that IT security has been infringed, penetrated or violated in anyway.

RESOURCES AND SYSTEMS COVERED BY THIS POLICY

This policy governs all IT resources and communications systems owned by or available at the Pendragon Group, and all use of such resources and systems when accessed using a team member's or third party's own resources, including but not limited to:-

- E-mail systems and accounts.
- Internet and Intranet access.
- Telephones and voicemail systems, including wired and mobile phones, smartphones and tablets.
- Printers, photocopiers and scanners.
- All other associated computer, network and communication systems, hardware, peripherals, and software, including network key fobs.
- Closed circuit television (CCTV) and all other physical security systems and devices, including access key cards and fobs.

NO EXPECTATION OF PRIVACY

All contents of the Pendragon Group's IT resources and communication systems are the property of the Pendragon Group. On this basis, team members and third parties should have no expectation of privacy whatsoever in any message, file, data, document, facsimile, telephone conversation, social media post, conversation or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on the Pendragon Group's electronic information and communications systems.

Team members and third parties are expressly advised that to prevent against misuse, the **Pendragon Group reserves the right to monitor, intercept and review, without further notice, every team member's or third party's activities using our IT resources and communications systems, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages and internet and social media postings and activities, and 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, intercepting, 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.

NETWORK SYSTEMS

The Pendragon Group maintains integrated computer and data communications networks to facilitate all aspects of its business. Team members must never sign onto any network equipment using the password, login or user name of another team member. No team members should access, attempt to access, alter or delete any network document except in furtherance of Pendragon Group business and where expressly authorised to do so.

DOWNLOADING AND INSTALLING SOFTWARE/WEBSITE AGREEMENTS

Email and downloading from the internet are prime sources of viruses and other malicious software. Team members may not download or install any software or shareware to their hard drive or any other Company IT systems that is not expressly approved or authorised by Pinewood Technologies Plc, and computer software is only to be installed Pinewood Technologies Plc In addition, team members or third parties may not accept the terms and conditions of website agreements without first obtaining approval from the Legal Department in accordance with the Company's Authority to Sign Documents and Contracts Policy as published on the Pendragon PLC intranet.

CONFIDENTIALITY AND PROPRIETARY RIGHTS

Pendragon and the Pendragon Group's confidential information and intellectual property should be never be jeopardised by a team member's or third party's personal use of electronic communication systems, including text messaging, internet access, social media and telephone conversations and voicemail. Disclosure and use of Pendragon Group confidential information and intellectual property is strictly prohibited. Team members and third parties are reminded that newsgroups and chat rooms are public forums where it is inappropriate to reveal any confidential information or discuss the business and affairs of the Company. Team members and third parties are prohibited from using any of the Pendragon Group's company names, trading names or styles, brand names, logos, taglines, slogans or other trade marks without express written permission from the Legal Department.

Team members and third parties are also prohibited from using the Pendragon Group's IT resources and communication systems in any manner that would infringe or violate the proprietary rights of others, including but not limited to copyrights, patents and design rights (both registered and unregistered). Team members should not knowingly use or distribute any such material downloaded from the intranet or received by e-mail without the prior written permission of the Legal Department.

E-MAIL AND TEXT MESSAGING

The Pendragon Group provides certain team members with access to e-mail and/or text messaging systems for use in connection with performance of their role. We seek to provide stable and secure email and text messaging systems (including SMS and internet-based instant messaging) with rapid, consistent delivery times that promote communication for business purposes without incurring unnecessary costs or generating messages that are unproductive for the recipient. The e-mail policies described below governing use of our e-mail and text messaging systems are aimed at reducing the overall volume of messages flowing through and stored on our networks, reducing the size of individual messages and making the system more efficient and secure.

Spam : Users of email and text messaging will occasionally receive unsolicited commercial or bulk messages (often referred to as spam), which aside from being a nuisance to team members and taking up IT resource, might be a means to spread computer viruses and other malicious software (malware). Team members must avoid opening unsolicited messages or clicking on links within such messages. Any suspicious messages must be reported to Pinewood Technologies PLC immediately. Do not reply to spam messages in anyway, even to state that you are requesting to be removed from a distribution list. If delivery persists, contact Pinewood Technologies PLC/technical support on who will block any incoming message from that address.

Team members should be aware that spammers often have the ability to access email addresses that are listed as senders or recipients on email messages, on websites, user discussion groups and other internet areas. Team members should be cautious about using and disclosing Pendragon Group e-mail addresses.

Etiquette : Proper business etiquette should be maintained when communicating via email and text messaging. When writing business email, be as clear and concise as possible. Sarcasm, poor language, inappropriate comments, attempts at humour and so on should be avoided. Email communications should resemble typical professional and respectful business correspondence. Email signatories and sign off should be accordance with approved Pendragon Group sign off; use of alternative font styles, colours and signatures is prohibited.

Personal Use of Pendragon Group provided email : The Company does allow the limited personal use of its e-mail systems, provided that such personal use does not interfere in any way with business use of its IT resources and communication systems and does not jeopardise the operation or integrity of the same. Team members should only use IT resources and communication systems for personal use out of necessity, and at all times in accordance with the Acceptable Use Principle as detailed in this policy. .

INTERNET AND SOCIAL MEDIA

We provide desktop internet access to certain team members for use in connection with the performance of their job role. Our expectations regarding internet use by team members are detailed below:-

Personal use of the internet : We allow team members to access the internet for personal use, provided that such personal use does not interfere in any way with business use of its IT resources and communication systems and does not jeopardise the operation or integrity of the same. Team members should only use IT resources and communication systems for personal use out of necessity, and use of the internet during business hours should at all times be conducted in accordance with the Acceptable Use Principle as detailed in this policy. Remember that we expressly reserve the right, without further notice, to monitor and review records of websites visited by team members, any postings or downloads made by team members whilst visiting websites as detailed under “No Expectation of Privacy” as above.

Use of Social Media : Use of social media is governed by the Company’s separate Social Networking Sites Policy.

TELEPHONE AND VOICEMAIL

We provide landline and or mobile telephone access and voicemail systems to certain employees for use in connection with performing their job role. To ensure that our customers and those with whom we do business with are provided with courteous and respectful service, and to prevent misuse of the Company’s IT resources, telephone conversations and voicemail messages of every team member may be monitored, recorded and reviewed. We may also store recorded telephone conversations and voicemail messages for a period of time after they take place, and may delete such recordings from time to time.

Personal use of telephony systems : We recognise that team members may occasionally need to use company landline or mobile telephones and voicemail for personal use provided that it does not interfere with your employment responsibilities or productivity. Our telephones must not be used for commercial, religious or political solicitation, or to promote outside organisations.

SAFEGUARDING ACCESS TO WORKSTATIONS, TABLETS AND OTHER IT EQUIPMENT

Team members or third parties must not leave computers, tablets and other IT equipment unattended without locking the screen or ensuring appropriate password protection is in place.

STATUS OF THE POLICY

This policy is adopted by the Company. It may be varied or withdrawn at any time, in the Company’s absolute discretion.