PENDRAGON

ACCEPTABLE USAGE POLICY 2023-2024.

Pendragon PLC, together with its affiliates and subsidiary companies, which includes our businesses trading as Evans Halshaw, Car Store and Stratstone (together, “Pendragon”, the “Company”, “we”, “us” or “our”) are committed to protecting the security of our customers, Associates, suppliers, online visitors and other third parties during the course of our activities. We have adopted this Acceptable Use Policy (the “Policy”) setting out the requirements and principles through which we seek to minimise the risks associated with accidental or malicious abuse of the equipment, information and services provided by Pendragon.

CONTEXT

We provide and consume a variety of services, conducting business online, via telephony and face to face. This Policy is designed to defend against constantly evolving threats that may reduce our ability to protect our customers, Associates and third parties, maintain business operations and impact our brand and reputation.

E-mail messages created by Associates may be disclosed to third parties either by accident or as a result of a court order and therefore must at all times be courteous, professional and business-like.

All information transmitted through or stored on the Company’s computer system, including e-mail messages, instant messages and conferencing services, is regarded as being the Company’s business information and at all times remains the property of the Company. The Company may at any time access, review, copy, modify and delete any information, including e-mails, in the computer systems.

- Use of Internet/intranet, instant messaging, voice and video conferencing and email will be subject to monitoring for security and/or network management reasons. Associates may be subject to limitations on their use of such resources.
- Information distributed through the Internet, computer based services, email and voice, video and instant messaging systems may be monitored by the Company. The Company reserves the right in its absolute discretion to determine the suitability of such information and its distribution.
- Any use of computing resources which is believed or suspected by the Company to be illegal or unlawful will be dealt with as the Company considers appropriate which may include reporting the incident to the appropriate authorities.
- Associates must take care when addressing e-mails to make sure messages are not sent to the wrong person.
- Distribution lists must be regularly reviewed and updated.

DEFINITIONS USED IN THIS POLICY

The definitions used in this Policy include:

Associates, defined as employees, temporary staff, and contractors.

AUDIENCE

In this policy, Pendragon aims to set out the standards of conduct expected by all of its Associates. This policy applies to anyone who has been given access to Pendragon owned electronic equipment or who represents Pendragon in any capacity.

For the purpose of this Policy, any tangible electronic devices owned by Pendragon such as iPads, iPods, Laptops, PCs, Mobile Phones and Printers will be referred to as “electronic devices”. This list is not intended to be exhaustive.

ENFORCING THIS POLICY

If you breach this Policy, you may be dealt with under Pendragon’s Disciplinary Policy, which could result in disciplinary action up to and including dismissal. If any of these breaches are of a criminal nature, Pendragon reserves its right to prosecute you under these circumstances.

As part of standard operation, Pendragon may monitor emails, Microsoft Teams, internet traffic, and video/voice calls to maintain security and protect confidentiality. By using the services provided by Pendragon you acknowledge your communications may be monitored.

GENERAL AND PERSONAL USE

Use of Pendragon’s internet, systems and services, including but not limited to voice and video conferencing, collabortation and email, is intended for business use. Personal use is permitted where such use does not affect the individual’s business performance, does not create a conflict of interest, is not detrimental to Pendragon in any way, is not in breach of any term and condition of employment and does not place the individual or Pendragon in breach of statutory or other legal obligations.

- Pendragon defines acceptable business use as activities that directly or indirectly support the business of Pendragon, its affiliates and subsidiary companies.
- Pendragon defines acceptable personal use on company time as reasonable and limited personal communication or recreation.
- Associates must not use their Pendragon email address to register for non-work related services, such as personal social media, online shopping or payment service accounts.
- Associates are blocked from accessing certain websites at the discretion of Pendragon. Such websites include, but are not limited to:
  - Adult and Pornography/Sexually Explicit, Criminal Activity, Gambling, Hacking, Illegal Drugs, Intolerance and Hate, Peer to Peer, Proxies and Translators, Discriminatory, Fraudulent, Tasteless and Offensive, Violence and Weapons.
  - The absence of blocking to sites that would fall into the above categories does not constitute approval for access. Any suspected omissions from blocking should be reported to Pendragon IT.
- Devices connected to Pendragon’s network should not be used to:
  - Store or transmit illicit materials.
  - Store or transmit proprietary or copyrighted information belonging to another company or individual.
  - Harass others.

- Associates must take care when opening emails and links, or responding to messages received, both from known and unknown sources. Whilst every effort is made to block suspicious communications, it is still possible that messages purporting to come from a trusted sender may still be successfully delivered.
- Associates must not enter into or indicate willingness to enter into a binding contract with any third party, unless expressly authorised to do so.
- Report any suspected or actual beaches immediately.

ACCOUNTS, PASSWORDS AND CLEAR DESK AND SCREEN

User accounts and associated passwords provide protection against unauthorised access:

- Associates must not distribute their username and passwords to other members of the Team unless in exceptional circumstances. Where required this must be agreed with a Team Leader.
- Examine, change, or use another Associate's files or output (other than those shared for collaboration or as part of day-to-day responsibilities) or username without explicit authorisation from a duly authorised Director or Team Leader to do so.
- Associates must ensure passwords are not easily guessable and adhere to the following:
  - Be a minimum length of eight (8) characters.
  - Not be a dictionary word, post code or proper name .
  - Not be the same as the User ID.
  - Contain mixed case, numbers and a special character.
- Where PINs are utilised, these must adhere to the following:
  - Be a minimum length of four (4) digits.
  - Not be any part Associate's date of birth or employee number.
  - Not contain consecutive or duplicate numbers.
- Associates must not write down passwords or store them in any other accessible form.
- All usage allocated to usernames/log-ins or passwords will be attributed to the account owner.
- Associates must report to Pendragon IT should they become aware that an account password has been compromised.
- Associates are provided with only the access they require to perform their job role. Should this not be the case, Associates must report this to their Team Leader.

In order to further reduce the risk of unauthorised access or loss of information, Pendragon enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers and portable devices must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Portable devices must also be physically secured when unattended, such as in a locked drawer or through security locks attached to a securing point.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

SOCIAL MEDIA AND MEDIA CONTENT

All Associates are accountable for their actions on the internet. Associates must not:

- Place any information on the Internet that relates to Pendragon, alter any information about it, or express any opinion about Pendragon, unless they are specifically authorised to do this.
- Make official commitments through the internet, or email, on behalf of Pendragon unless authorised to do so.

SOFTWARE AND CLOUD SERVICES

Associates must use only software and cloud services that are provided by Pendragon on Pendragon's computers.

Associates must not:

- Store Pendragon information on any cloud service other than those provided by Pendragon.
- Use backup, synchronisation, or any software designed to store files on cloud service, other than those provided by Pendragon.
- Store personal files such as music, video, photographs or games on Pendragon's electronic equipment, servers or cloud services.
- Intentionally interfere with the normal operation of the network and systems, including the propagation of computer viruses and sending high volume network traffic that substantially hinders other Associates in their use of the network.
- Use third party communication services to discuss, communicate or transfer information classified as confidential or above that have not been approved by the Company, such as Whatsapp.

Associates must utilise the Company's approved video conferencing service, Teams, for all internal meetings, ensuring We can protect Company information at all times. The Company's Teams service should also be the default service used for all external meetings, wherever possible.

DATA SECURITY

Securing Pendragon's data is critical to protect our customers, our business and in meeting our regulatory obligations. Associates must consider the sensitivity of information and how to protect it during collection, processing, storage and transmission.

Associates must not:

- Send unprotected sensitive or confidential information externally.
- Forward Pendragon mail to personal non-Company email accounts (for example a personal Hotmail account).
- Use removable media devices other than those authorised by Pendragon, meeting requirements such as encryption and management.
- Remove, reconfigure, or in any way tamper with security controls in use within Pendragon's network and upon electronic devices.
- Software must be used in accordance with the software supplier's licensing agreements.
- All software on Pendragon's computers must be approved and installed by Pendragon's IT department.

REMOTE WORKING

Pendragon provides mobile working solutions that must be used if working remotely from our offices. When working remotely Associates must:

- Only access Pendragon application and services via authorised devices, such as company provided laptops or desktops.
- Not forward Pendragon mail to personal non-Company email accounts (for example a personal Hotmail account).
- Use privacy screens when accessing sensitive or confidential information (for example customer information or company reports) in public areas or where they may be overlooked by non-company individuals;
- Ensure electronic devices used to access Pendragon information are secured when not in use:
  - Ensure screens are locked when unattended, requiring a password to log back in;
  - Shut down devices at the end of the working day, and before any travel;
  - Do not leave devices in vehicles overnight and ensure they are out of sight when travelling by car, left at home, or in hotel rooms.
- Avoid making hard copies or manual notes containing sensitive or confidential information (for example customer information or company reports). Where this can not be avoided:
  - Lock away materials containing sensitive or confidential information (for example customer information or company reports) when not in use;
  - Ensure materials containing sensitive or confidential information are disposed of securely, through confidential waste bins available in Pendragon offices.
- Not take customer calls, which entail customer data, in public areas or areas where they can be overheard by noncompany individuals;
- Not use non company services or software for online meetings.

PERSONAL DEVICES AND PHOTOGRAPHY

The use of personal devices is permitted in certain circumstances. Associates must not:

- Connect any personal devices to Pendragon's network.
- Use any personal electronic equipment during working hours in view of our customers.
- Take photographs of the exterior or interior of your workplace, unless authorised to do so.
- Upload or email any authorised photographs to any internet website, blog, social networking site or similar site unless the purpose of posting the pictures is for marketing purposes or to promote the business.
- Take any photographs where the resulting photographs (including the subject matter of the photograph and surrounding background) would pose a risk to the confidentiality, privacy or dignity of the company, its Associates, suppliers or customers, or where any such photographs are likely to cause anyone offence.

SUPPORTING DOCUMENTS

The following documents support the implementation of this Policy and its requirements:

- Information Security Policy.
- Data Protection Policy.

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. We encourage you to regularly check our website for any updates or changes to this policy.