Information Technology Access & Security Policy

(Version 2026)

Revision History

REVISION	DATE OPERATIONAL	CEO/BOARD APPROVAL	NEXT REVIEW	PREPARED BY
2018.A	01/07/2018	01/07/2018	01/07/2019	Mr. S. Shahi, Group IT Manager
2020	17/08/2020	03/08/2020	07/2022	Mr. S. Shahi, Group IT Manager
2022	01/04/2022	31/03/2022	07/2024	Mr. S. Shahi, Group IT Manager
2023	01/08/2023	01/08/2023	08/2024	Mr. S. Shahi, Group IT Manager (Urgent Changes)
2024	07/01/2025	07/01/2025	01/2026	Mr. S. Shahi, Group IT Manager
2026	15/01/2026	15/01/2026	01/2027	Mr. S. Shahi, Group IT Manager

Introduction

The Information and Communication Systems are an integral part of the business at White and Company PLC. The company has made a substantial investment in human and financial resources to create these systems. This policy has been created to:

- Protect these investments
- Safeguard the information stored within these systems
- Minimise business and legal risks
- Prevent reputational damage to the company and its employees
- Ensure the Health and Safety of all staff

Violations

Violating the policies outlined in this document may result in disciplinary actions as per company policy. The severity of the action depends on the nature and extent of the violation, any resulting harm to the company, and the recurrence of such violations. In cases involving harm to staff or customers, local law enforcement may be involved.

Administration

The administration and enforcement of this policy falls under the responsibility of the Group Information Technology Manager (Group IT Manager).

Contents

This document covers the following topics:

1. Statement of Responsibility
2. Internet Usage, World Wide Web (WWW), and Cloud
3. Malware and Cyber-Incidents
4. Social Networking
5. Multi Factor Authentication (MFA) and Passwords
6. Physical Security
7. Personal Mobile Devices
8. Data Backup
9. Copyrights and License Agreements
10. Personal Data and GDPR
11. Use of Generative AI (Artificial Intelligence)

1. Statement of Responsibility

Manager Responsibilities

Branch Managers, Department Heads, and Supervisors are required to:

- Ensure all relevant personnel are aware of and comply with this policy
- Monitor compliance and take action if employees fail to adhere to the policy

The Group IT Manager is responsible for:

- Developing and maintaining standards and procedures to ensure the effective implementation and adherence to the policy
- Providing support and guidance to employees in fulfilling their responsibilities under this policy

2. Internet, WWW, and Cloud

The Internet, also known as the World Wide Web or Cloud, is a vast, publicly accessible network connecting billions of users and devices worldwide. It provides services like Email, Websites, Remote Servers, and Communication tools.

Policy

The Internet is a resource provided to employees to support the operations of White and Company PLC. While it offers valuable business tools, it also presents risks. To protect the company's interests, the following guidelines have been established for responsible use of Internet-based services.

Acceptable Use

Employees should use the Internet for business-related activities, including:

- Using email for communication and marketing
- Accessing business websites, hosted applications, and databases
- Connecting to remote company computers or partners' networks
- Using IP telephony, video communication, and collaboration tools

Unacceptable Use

Employees must not engage in activities such as:

- Sending or forwarding spam or malware-infected messages
- Accessing unauthorized or illegal websites
- Streaming media without authorisation
- Conducting personal business during work hours
- Sharing offensive or discriminatory content
- Accessing non-business related websites

Downloads

Employees must not download files or programs from the Internet without written authorisation from the IT Manager, except for email attachments or approved updates from trusted sources e.g. gov.uk, transfernow.net

Employee Responsibilities

- Ensure all Internet communications are professional and do not disrupt work productivity
- Take responsibility for any content sent over the Internet
- Must not transmit copyrighted material without permission
- Follow company policies regarding security, data protection, and confidentiality
- Use encryption and password protection when sending sensitive customer information

All communications over company systems and networks are monitored and logged. This includes all type of files, voice and video communications. The company reserves the right to access and disclose and share any files deemed necessary for business purposes and for law enforcement.

3. Malware and Cyber-Incidents

Malware refers to harmful software designed to damage systems or steal data. The resulting Cyber-Incidents pose a significant risk to the company's infrastructure and data. Such malware can be delivered using various mechanisms e.g. phishing, compromised websites, etc.

Background

Preventing malware infections is easier than dealing with the consequences. Key protections include secure access controls, trusted data sources, end-point security and management software.

Cyber Security Officer Responsibilities

The Cyber Security Officer, along with the Group IT Manager, must:

- Install and maintain endpoint protection software
- Maintain Web filtering software to mitigate access to non-business related and malicious websites
- Use Privileged Access Management for management of devices
- Monitor, respond to, and document security incidents per company policies
- Disseminate good practice and provide training resources for staff

Employee Responsibilities

- Avoid introducing malware to company systems
- Not use external storage devices unless authorised
- Scan all external devices for malware before use if authorised
- Report suspected malware infections immediately to the IT Team
- Immediately power off any suspect device
- Follow good practice guides including online mandatory Cyber Security training

4. Social Networking

This policy covers all social media platforms, including Facebook, Twitter, LinkedIn, Instagram, and others.

Employee Responsibilities

- Shall NOT disclose proprietary company information on social media without prior written consent

- Read and comply with the terms and conditions of social media platforms
- Avoid making defamatory comments about the company or its stakeholders
- Not use company devices to access social media unless authorised

Group IT Manager Responsibilities

- Maintain website filters to prevent unauthorised access to social media
- Monitor access and report any violations

5. Multi-factor Authentication (MFA) and Passwords

The confidentiality and integrity of data stored on systems must be protected by suitable access controls for authorised employees. As a result, access will be restricted to data that is required for the employee's job role. All Users will have both sign-on credentials and a unique MFA code.

Group IT Manager Responsibilities

The IT Manager and his team are responsible for managing access controls and processing access requests from managers or department heads.

Employee Responsibilities

- Never share passwords and update them regularly
- Store passwords securely, using encryption
- Use complex passwords (at least 10 characters with letters, numbers, and symbols)
- Log out or Lock the workstation when leaving your working area
- Report any suspicious activity to the IT team

Manager Responsibilities

Managers must notify the IT team, immediately, when an employee leaves or transfers, to revoke or modify access.

6. Physical Security

The company ensures that all IT equipment is protected from theft, unauthorised access, and environmental hazards.

Employee Responsibilities

- Use only company-approved encrypted storage devices if authorised
- Avoid environmental hazards like food, liquids, and extreme temperatures
- Report any equipment issues to the IT department ASAP

7. Personal Mobile Devices

The company does not support the use of personal devices for business purposes, except for specific applications such as ID verification and communication apps. Personal devices include phones, tablets, smart wearables. Smart wearable devices e.g. Smart Glasses, that can capture audio, video and those devices that can interfere with Health & Safety requirements are forbidden to be used in

the workplace (this includes any Whitport owned company), company vehicles, customer sites as these can impact the privacy, security and safety of the company, staff, and customers.

8. Data Backup

The company maintains regular backups of critical data, including emails and key databases, both on-site and off-site for disaster recovery.

Employee Responsibilities

- Store Moveware related files and emails within the Moveware Documents folder structure
- Other critical files on server mapped drives and/or shared folder locations
- Must not store critical files on the local disks of their personal computer

9. Copyrights and License Agreements

Employees must comply with copyright laws and only use licensed software on company systems.

Employee Responsibilities

- Only install authorised software on company devices
- Do not download or copy software without permission

10. Personal Data and UK- EU GDPR

The company adheres to all relevant data protection regulations, including UK DUAA 2025, EU GDPR, to safeguard employee and customer data.

Employee Responsibilities

Employees must protect personal data and comply with the company data privacy and protection policies.

11. Use of Generative AI (Artificial Intelligence)

The use of generative AI technologies is strictly prohibited within the company IT environment and during the course of any official duties unless authorised by the Cyber Security and Data Protection officers. This restriction includes, but is not limited to:

Employee Responsibilities

- Employees (or contractors) must not access or utilise generative AI tools, including but not limited to ChatGPT, DALL·E, Stable Diffusion, or similar platforms, on company devices or networks unless authorised.
- Employees (or contractors) are strictly prohibited from submitting/uploading any company, customer, or partner-related data or information whether confidential or not to generative AI platforms.
- Authorised employees must have suitable training and guidance from the Cyber Security and Data Protection officers.

The company recognises the potential benefits of generative AI technologies; however, their use presents significant risks, including:

- Generative AI tools store and potentially analyse user-submitted data, creating a risk of unintentional data exposure or misuse.
- Submitting sensitive or regulated information to external AI platforms may result in breaches of legal and contractual obligations, including but not limited to GDPR, CCPA, or industry-specific regulations.
- The use of unauthorised AI tools may increase the risk of introducing vulnerabilities, malware, or unverified outputs into the company systems.

Acknowledgment of Information Technology Access & Security Policy

Summary - Employee Responsibilities

- Ensure that all communications are for professional reasons and that they do not interfere with their productivity.
- Shall be responsible for the all documents, audio and video content that they store or send over the Internet.
- Not transmit copyrighted materials without permission.
- Know and abide by all applicable White and Company PLC policies dealing with security, data protection and confidentiality of data (company or customer).
- Avoid transmission of non-public customer or company information unless necessary in which case reasonable steps must be taken to secure such information using passwords, encryption and confirmation that any delivery target is authorised to receive such information.
- Not knowingly introduce computer malware onto company computers/smart devices.
- Shall IMMEDIATELY POWER OFF their computer and call the IT Support Team if suspecting that their computer has been infected or has been compromised (Unauthorised Access).
- Shall NOT grant remote access to their computer systems other than to members of the IT Team or as directed by the IT Team.
- Must exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.
- Shall NOT access 'Social Networking' sites using company equipment without written consent from the IT Manager.
- Shall NOT Install software either directly or by a third party unless authorised by the IT Team. Only software that is licensed or owned by White and Company PLC is to be installed on company computers, tablets and smart devices.
- Shall NOT download files, documents from unauthorised sites unless agreed by the IT Team.
- Shall not utilise generative AI or upload any data to any AI platforms unless authorised.

By signing below, I agree to the following terms:

1. I have received and read a copy of the "Information Technology Access & Security Policy" and understand the same;
2. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about White and Company PLC (& Whitport Group of Companies) its customers or its vendors, and that this is and remains the property of the company at all times;
3. I agree that I shall not copy, duplicate (except for backup purposes as part of my job at White and Company PLC), or disclose company /personal data or software held on company servers and computers to unauthorised individuals;
4. I agree that, if I leave White and Company PLC, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

Employee Signature: _____

Employee Name: _____

Date: _____

Branch/Department: _____