Form Title: Cyber Security Policy
Form Ref: POL 025
Author: PRB Consulting
Date: June 2025
Version: V2.0

CYBER SECURITY POLICY

PURPOSE
This Cyber Security Policy sets out how Role Group Ltd / Role Training Ltd protects its information, systems, and data from cyber threats, unauthorised access, and data breaches.

We are committed to ensuring the security and integrity of all data in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

2. SCOPE
This policy applies to:
- Employees
- Contractors
- Temporary staff
- Any individual with access to company systems or data

3. CONFIDENTIAL DATA
Confidential data includes, but is not limited to:
- Financial information
- Customer, supplier, and partner data
- Employee data
- Commercial or proprietary information

All individuals must ensure this data is protected from unauthorised access, disclosure, loss, or misuse.

4. RESPONSIBILITIES
Employees
Employees must:
- Follow this policy at all times
- Report security incidents immediately
- Protect company systems and data

Management
Management is responsible for:
- Ensuring security controls are implemented
- Supporting staff training
- Responding to cyber incidents

IT Provider (MaptecIT)
The IT provider is responsible for:
- System security and maintenance
- Monitoring threats
- Responding to incidents
- Advising on cyber risks

5. DEVICE AND SYSTEM SECURITY
Employees must ensure that all devices used for work purposes are secure:
- Devices must be password protected
- Systems must be locked when unattended
- Security updates must be installed promptly
- Antivirus and firewall protections must be active
- Company systems must only be accessed via secure networks
- Accessing company systems on shared or public devices is prohibited unless authorised.

6. PASSWORD MANAGEMENT
Passwords must be:
- Strong (minimum 12 characters recommended)

- Unique and not reused across systems
- Kept confidential at all times

Employees must not share passwords.
Where available, **multi-factor authentication (MFA)** must be used.
Password managers may be used if approved by IT.

7. EMAIL AND PHISHING SECURITY
Employees must take care when handling emails:

- Do not open suspicious attachments or links
- Verify sender details before responding
- Report phishing attempts immediately

Common warning signs include:

- Unexpected attachments
- Poor grammar or urgent requests
- Requests for passwords or sensitive data

8. DATA TRANSFER AND STORAGE
Sensitive data must be handled securely:

- Only share data where necessary and authorised
- Use secure company systems for data transfer
- Do not use public Wi-Fi for transmitting sensitive data
- Ensure recipients are authorised

Personal data must be handled in accordance with the **Data Protection Policy**.

9. INTERNET AND SOFTWARE USE
Employees must not:

- Access illegal, inappropriate, or harmful websites
- Download unauthorised software
- Install applications without approval

All software must be approved by management or the IT provider.

10. MONITORING AND SECURITY CONTROLS
Monitoring
The Company may monitor IT systems to:

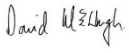
- Detect unauthorised use
- Prevent cyber threats
- Investigate incidents

Lawful Basis
Monitoring is conducted under **UK GDPR Article 6(1)(f) – Legitimate Interests**, to protect:

- Company systems
- Personal data
- Business operations

POLICY REVIEW

This policy will be reviewed annually and updated as required to reflect legal, regulatory, or operational changes.

Signed 

David McHugh
Managing Director
June 2026