Policy Title: IT and Communications Policy
Policy Ref: POL 024
Author: R Bell
Date: June 2026
Version: V6.0

IT & COMMUNICATIONS SYSTEMS POLICY

1. ABOUT THIS POLICY

Our IT and communications systems support effective communication and business operations. This policy outlines acceptable use, monitoring, and responsibilities when using company systems.

Breaches of this policy may result in disciplinary action under the Company's Disciplinary Procedure and may constitute gross misconduct.
This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy is aligned with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and relevant ICO guidance.

2. EQUIPMENT SECURITY AND PASSWORDS

Employees are responsible for all equipment issued to them and must ensure it is used securely.
Strong passwords must be used and kept confidential. Passwords must not be shared.
Systems must only be accessed using authorised login credentials.
Devices must be locked when unattended and fully logged out/shut down at the end of each working day.

3. SYSTEMS AND DATA SECURITY

You must not modify, delete, or interfere with systems or data unless authorised.
Unauthorised software must not be installed.
External devices (USBs, phones, tablets) must not be connected without approval.
All emails are scanned for security threats. Exercise caution with unknown or suspicious emails.
Any suspected cyber incident (including viruses or phishing) must be reported immediately to management.

4. E-MAIL USE

Use a professional tone in all communications.
Emails are business records and may be accessed for legitimate purposes.
The following is strictly prohibited:

- Offensive, abusive, or discriminatory content
- Harassing or defamatory messages
- Inappropriate or unlawful material

Employees must not:

- Send chain mail, spam, or non-business content
- Use another person's email account without authorisation
- Send business emails from personal accounts

Personal email services (Gmail, Hotmail etc.) must not be accessed on company systems unless authorised.

5. INTERNET USE

Internet access is primarily for business purposes.
Employees must not access or download content that is:

- Illegal
- Offensive or discriminatory
- Inappropriate or likely to cause reputational damage

The Company reserves the right to restrict access to certain websites.

6. PERSONAL USE

Limited personal use is permitted but must be minimal and must not interfere with work duties.
Personal use must:

- Occur mainly outside working hours (e.g. breaks)
- Not impact productivity or system performance
- Comply with all company policies

Personal use is a privilege and may be withdrawn.

7. MONITORING AND PRIVACY

Monitoring Statement

The Company reserves the right to monitor the use of its IT and communication systems, including:

- Emails
- Internet usage
- Telephone systems
- Other electronic communications

Lawful Basis

Monitoring is carried out in accordance with **UK GDPR Article 6(1)(f) – Legitimate Interests**, including:

- Ensuring compliance with company policies
- Preventing misuse and protecting systems
- Investigating incidents or misconduct
- Meeting legal and regulatory obligations

Proportionality

Monitoring will be:

- Proportionate
- Necessary
- Carried out in line with data protection principles

A **Legitimate Interest Assessment (LIA)** and **Data Protection Impact Assessment (DPIA)** are in place where required.

8. PROHIBITED USE

Misuse of company systems may result in disciplinary action.
The following are strictly prohibited and may constitute **gross misconduct**:

- Accessing pornographic material
- Viewing or distributing offensive, discriminatory, or abusive content
- Sharing confidential company or client information without authorisation
- Installing unauthorised software
- Downloading copyrighted material without permission
- Any activity that may expose the company to legal or reputational risk

9. DATA PROTECTION RESPONSIBILITIES

Employees must comply with the Company's **Data Protection Policy** when handling personal data.
Personal data must:

- Be processed lawfully, fairly, and transparently
- Be kept secure
- Not be shared without authorisation

10. REPORTING CONCERNS

Any concerns regarding IT use or security incidents must be reported immediately to management.

11. COMPLAINTS

Employees may raise concerns via:

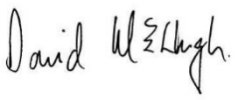
Email: training@rolegroup.co.uk

Alternatively, complaints can be made to the Information Commissioner's Office (ICO):

- Website: https://ico.org.uk
- Helpline: 0303 123 1113
- Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

12. POLICY REVIEW

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

Signed: 

Role: Managing Director

Date: June 2026