Mobile Phone & Laptop Acceptable Use Policy

ADR Carriers Limited

Company details
ADR Carriers Limited
Church View, Newton Arlosh
Wigton, Cumbria
CA7 5ET

Company Number: **14798586**
Email: **hazload@adrcarriers.net**

---

1. Purpose

This policy sets out the rules for the use of mobile phones, laptops, and other portable computing devices used for ADR Carriers Limited business, to protect company information, personal data, and IT systems.

---

2. Scope

This policy applies to:

- All employees, directors, contractors, and agency staff
- All company-issued and personally owned devices used for company business
- Mobile phones, laptops, tablets, and similar portable devices

---

3. Acceptable Use

Devices may be used for legitimate business purposes, including:

- Communication with customers, suppliers, and colleagues
- Accessing company systems and documentation
- Navigation, compliance, and operational applications

Limited personal use is permitted provided it does not interfere with work duties or compromise security.

---

4. Security Requirements

All devices used for company business must:

- Be protected by a strong PIN, password, or biometric security
- Automatically lock when not in use
- Use up-to-date operating systems and security patches
- Have antivirus and malware protection where applicable

Company data must not be stored on unsecured or shared devices.

---

5. Data Protection & Confidentiality

Users must:

- Handle personal and confidential data in accordance with UK GDPR
- Avoid accessing or displaying sensitive information in public places
- Ensure devices are not left unattended in insecure locations
- Use secure networks; public Wi-Fi should be avoided or used only with appropriate safeguards

---

6. Email, Messaging & Communications

- Company email accounts must be used for business communications
- Personal email or messaging apps must not be used to transmit company or personal data unless authorised
- Users must remain vigilant against phishing and malware

---

7. Loss, Theft or Damage

Any loss, theft, or suspected compromise of a device must be reported immediately to:
hazload@adrcarriers.net

Prompt reporting enables remote security measures and breach assessment.

---

8. Software & Applications

- Only authorised software and applications may be installed
- Users must not bypass security controls or install unapproved apps
- Cloud storage services must not be used unless approved by ADR Carriers Limited

---

9. Personal Devices (BYOD)

Where personally owned devices are used for company business:

- Company data must be kept separate from personal data
- Security requirements in this policy still apply
- The Company reserves the right to require removal of company data

---

10. Monitoring

ADR Carriers Limited reserves the right to monitor the use of company devices and systems for security, compliance, and operational purposes, in accordance with applicable law.

---

11. Disciplinary Action

Failure to comply with this policy may result in disciplinary action and may lead to termination of access or contractual consequences.

---

12. Responsibilities

All users are responsible for:

- Following this policy
- Protecting company and personal data
- Reporting security incidents promptly

---

13. Review

This policy is reviewed regularly and updated as required.

Last reviewed: December 2025
Next review: December 2026
