Information Security Policy

Public summary of information security policy.

Company	Pariter Limited (company number 05308864)
Registered office	5/6 Salmon Fields Business Village, Oldham, Lancashire, OL2 6HT
Policy owner	Ian Chadwick, Director
Contact email	info@partier.co.uk
Version/status	Version 0.1 | Draft for internal approval and website publication
Review cycle	Approved on [INSERT APPROVAL DATE]; review at least annually or sooner following legal, regulatory or operational change.

1. Policy statement

Pariter Limited is committed to protecting the confidentiality, integrity and availability of information entrusted to it by clients, staff, suppliers and other stakeholders. This public policy summarises our information security approach without disclosing detailed security controls.

2. Scope

This policy covers business information, personal data, project records, client reports, commercially sensitive information, professional advice, financial information, IT systems, cloud services, devices and communications.

3. Core controls

- Access to systems and information should be limited to authorised users with a business need.
- Users should use strong authentication and keep passwords, credentials and devices secure.
- Confidential information should be stored in approved systems and shared only through appropriate channels.
- Portable devices and remote working arrangements should be protected against loss, theft and unauthorised access.
- Suppliers handling confidential information or personal data should be assessed proportionately and bound by suitable contractual obligations.
- Security incidents, suspected phishing, lost devices and unauthorised disclosures should be reported promptly.

4. Data handling

Information should be classified and handled according to sensitivity. Project documents, reports, personal data, confidential client information and commercially sensitive information should not be disclosed unless authorised, lawful and necessary.

5. Incident response

Security incidents will be assessed, contained and investigated. Where an incident involves personal data, Pariter Limited will assess whether notification to the Information Commissioner's Office, affected individuals, clients, insurers, RICS or other parties is required.

6. Business continuity

Pariter Limited will take proportionate steps to maintain continuity of critical systems and records, including backups, recovery arrangements and supplier resilience considerations.

7. Responsibilities

All staff and suppliers handling Pariter Limited information are responsible for following security requirements, reporting incidents and using information only for authorised business purposes.

Review and approval

This document is owned by Ian Chadwick, Director. It should be reviewed at least annually, and whenever Pariter Limited changes its services, suppliers, cookie technology, personal data uses, RICS registration arrangements, complaints procedure, ADR provider, insurance arrangements or client money arrangements.

Version	Date	Approved by	Changes
0.1	11 May 2026	[INSERT APPROVER]	Initial draft for website policy suite.