MANDOLAY

One Unique Hotel
Infinite Possibilities

Cybersecurity Policy

Introduction

Welcome to The Mandolay Hotel's cybersecurity policy. The Mandolay Hotel is the trading
name of the partnership of William Hay and Stephen Hay of The Mandolay Hotel, 36-40 London Road, Guildford, GU1 2AE ("The Hotel").

The Hotel takes all aspects of security extremely seriously and is committed to protecting the personal data and on-line safety of our guests, patrons, and colleagues.

Please refer to our Privacy Policy for details of how we collect, store, and safely remove personal data.

Purpose. And Overview

This policy sets out how we protect our systems, data, and guests from cyber threats. It applies to all employees, contractors, and third-party partners.

Our Responsibilities

1. Passwords.

All appropriate staff and every manager receives training about the use of strong, unique passwords for each of our systems.

Multi-Factor Authentication must be enabled, and used where available.

Access is universally granted on a minimum necessary basis and is removed immediately when team members leave the employment of The Hotel.

2. Data Protection

As set out in our Privacy Policy, all data is handled in strict accordance with GDPR obligations.

Data must only be collected for the precise business use intended.

Data is stored securely, and safely removed when no longer required.

3. Testing

All staff are trained in email and phishing awareness, and The Hotel regularly undertakes rigorous testing of this policy. Where failings are detected, our policy dictates that additional training, and where appropriate enhanced supervision is provided.

All phishing attempts, or suspected phishing activity must be logged immediately and handled via our internal reporting system.

Mandolay employs the service of an IT service and as of January 2026, we are actively pursuing Cyber Essentials accreditation via a third party specialist provider.

4. Use of Devices

All systems must comply with approved security software.

The use of storage devices such as USB, or memory devices is strictly forbidden at every level up to Managing Director and Sales Director.

Our CCTV system is controlled in-house using a third party provider, with footage stored for a limited time. No footage is shared unless requested by the police, emergency services or representatives of HM Government.

5. Website Management

All content updates are handled in-house by a named senior manager.

All software updates and patches are managed by a trusted third party supplier, in strict accordance with our Privacy, GDPR, and Cybersecurity policies.

This policy is reviewed and updated at least annually, or should an incident occur, immediately thereafter.

For further information about this, or any other hotel policies please contact us via our website.

Matthew Milliken

Managing Director

January 2026