

# Acceptable Use Policy

Last updated: 21 July 2026

---

## 1. Purpose

This Acceptable Use Policy applies to the use of YachtCloud's website, software, apps, APIs, products, accounts, systems, support services, server-related services and related technologies. It is designed to protect YachtCloud, our customers, end users, systems, networks, data, product integrity, third-party services and the wider internet community.

This Acceptable Use Policy applies together with our Terms of Service, Privacy Policy, Cookie Policy, Refund and Return Policy, Shipping Policy, Software Licence Agreement, Service Level Agreement, Hardware Warranty Policy, Data Processing Agreement, and any quote, invoice, proposal, order form, support agreement or signed customer contract that applies to the relevant product or service.

Customers are responsible for their own actions and for the actions of their users, guests, staff, crew, contractors, visitors, service providers, integrators and any other person using the products through their account, system, licence or environment.

## 2. Fair and authorised use

You must use the products only for lawful, authorised and agreed purposes. Usage must remain within the scope of the applicable quote, licence, support plan, product documentation, technical requirements and customer agreement. Excessive use, misuse, unauthorised sharing, tampering or use beyond agreed limits may result in suspension, restriction, additional charges or termination.

## 3. Prohibited use

You must not use the products to:

- break any law, regulation, court order or third-party right;
- infringe intellectual property, privacy, confidentiality, publicity or data protection rights;
- upload, store, transmit, create or share illegal, harmful, obscene, defamatory, abusive, discriminatory, threatening or exploitative content;
- send spam, unsolicited bulk messages, unauthorised marketing messages, phishing messages or deceptive communications;
- access, test, scan, interfere with or attack any system, network, account, API, server, device or data without authorisation;
- introduce malware, viruses, malicious code, exploits, denial-of-service tools, credential harvesting tools or similar harmful technologies;

- bypass usage limits, licence limits, security controls, authentication controls, access restrictions or payment obligations;
- copy, modify, reverse engineer, tamper with, disable, remove notices from or interfere with YachtCloud software, hardware or systems except where expressly allowed;
- share credentials or allow unauthorised access to YachtCloud products;
- use the products for illegal gambling, terrorism, narcotics trafficking, arms trafficking, sanctions evasion, weapons development or other prohibited activities;
- use the products if you, your vessel, or any individual, entity or beneficial owner involved in your use of the products is designated on, owned by, controlled by, or acting on behalf of a party on, any applicable trade, economic or financial sanctions or restricted party list.

#### **4. APIs, integrations and third-party systems**

Where YachtCloud provides an API or integration capability, you may use it only within the agreed scope and in a way that does not harm YachtCloud, customers, end users, third-party platforms or connected systems. You must not overload, scrape, abuse, reverse engineer, bypass, attack or use integrations in a way that creates security, performance, privacy or legal risk.

#### **5. Customer data and content**

You are responsible for the accuracy, lawfulness, permissions, rights and legal bases for any data or content you upload, store, transmit, manage or process through the products, including guest data, crew data, visitor data, staff records, service requests, messages, images, videos, voice messages, location-related data, documents, NDAs, security forms, logs and operational data.

#### **6. Security responsibilities**

You must maintain appropriate security controls for your accounts, users, local devices, networks, servers, onboard systems, third-party accounts and access permissions. You must promptly notify YachtCloud if you become aware of unauthorised access, compromised credentials, misuse, suspected security incident or unauthorised product use.

#### **7. Confidentiality and restricted materials**

You must not disclose confidential YachtCloud materials, including pricing, credentials, system access details, security details, non-public technical information, project-specific configuration, support information or other confidential materials, except where authorised or necessary for the agreed project.

## **8. Operational and safety use**

YachtCloud products may support communication, service management, guest experience, internal organisation, visitor management, network access, media control, floor plan information, CCTV access or muster list workflows. They are assistive tools and must not be used as a replacement for crew responsibility, emergency procedures, safety systems, regulatory compliance, professional judgement, backup processes or manual controls.

## **9. Enforcement**

If we believe this policy has been breached, we may investigate, suspend access, restrict functionality, remove content, request remediation, notify the customer, terminate services, preserve records, cooperate with authorities or take any other lawful action we consider appropriate. Where legally required or necessary to protect safety, security or legal rights, we may act without prior notice.

## **10. Changes to this policy**

We may update this policy from time to time. Updated versions will be published on our website or made available through appropriate channels.

## **11. Contact**

For questions about this Acceptable Use Policy, contact YachtCloud at [support@yachtcloud.com](mailto:support@yachtcloud.com).