

CRM Platform Terms of Use and Data Responsibility Notice

For business clients using services delivered through HighLevel / LeadConnector or related third-party CRM and automation infrastructure

In this document, "Agency" means Your Golf Marketing Limited.

Prepared by	Your Golf Marketing Limited
Version	v1.0
Important	B2B use only.

Purpose of this document: to explain how the Agency delivers services through a third-party CRM platform, to clarify the Client's own compliance responsibilities, and to limit the Agency's liability in relation to platform use, client instructions, data inputs, and legal compliance.

This document is designed to sit alongside the Agency's wider services agreement, proposal, statement of work, or terms of business. Where there is any inconsistency between this document and a signed master agreement, the signed master agreement should prevail unless expressly stated otherwise.

References in this document to the "Platform" include HighLevel, LeadConnector, associated infrastructure, approved integrations, and any white-labelled environment through which the Agency provides CRM, forms, funnels, pipeline management, messaging, automation, reporting, or related services.

1. Scope and Acceptance

By instructing the Agency to set up, manage, or support the Platform, or by accepting access to, logging in to, accessing, or continuing to use the Platform, the Client confirms that it has read and accepted this document and agrees that these terms apply to all Platform-related services unless replaced by a separately signed agreement.

- The Platform is a third-party software environment. It is not owned or controlled by the Agency.
- The Agency may configure, manage, or support the Platform, but the underlying software, hosting, and many technical controls remain with the platform provider and its sub-processors.
- The Client acknowledges that features, workflows, integrations, user permissions, deliverability, retention settings, and compliance tools may change over time as the platform provider updates its systems.

2. Data Protection Roles

For most engagements, the parties agree the following applies unless expressly documented otherwise in writing:

Party	Likely role	Practical meaning
Client	Controller (or processor for its own customers)	The Client decides why data is collected, what data is collected, and how it is used in its business.
Agency	Processor / service provider	The Agency configures or manages the Platform on the Client's instructions and does not determine the Client's wider legal basis or compliance position.
Platform provider	Sub-processor / infrastructure provider	The platform provider hosts and operates the underlying system and may appoint approved sub-processors.

The Client remains responsible for ensuring that its use of the Platform is lawful in the jurisdictions in which it operates and for the categories of data it chooses to collect, upload, process, or communicate.

3. Client Responsibilities

The Client is solely responsible for:

- determining its lawful basis for collecting and processing personal data;
- publishing and maintaining an accurate privacy notice and any required disclosures;
- ensuring all forms, landing pages, booking journeys, and lead capture points use suitable consent language where required;
- keeping records of consent, including offline or verbal consent where applicable;
- responding to requests for access, erasure, rectification, objection, suppression, or portability;
- deciding how long data should be retained and ensuring a workable deletion process exists;

- reviewing whether a data processing agreement, internal policy update, or legal advice is required before launch;
- ensuring all campaigns, SMS, email, WhatsApp, call tracking, AI, and automation activity complies with applicable law.

The Agency may provide practical recommendations on setup and process, but the Client acknowledges that the Agency is not acting as the Client's solicitor, data protection officer, or regulated compliance adviser.

4. Restricted and Sensitive Data

Unless the Agency expressly agrees in writing and confirms that the proposed workflow is suitable, the Client must not use the Platform to collect, store, process, or transmit:

- full payment card details, card verification values, or unmasked bank account details;
- passport numbers, national insurance numbers, social security numbers, or equivalent government identifiers;
- special category or highly sensitive data, including detailed health data, biometric data, criminal offence data, or data concerning children;
- any data category that the Client is not lawfully entitled to collect or that requires additional controls which have not been implemented.

If the Client uploads or captures restricted data without prior written approval, it does so entirely at its own risk and shall be fully responsible for any resulting loss, claim, investigation, notification duty, fine, remediation cost, or third-party complaint.

5. Hosting, International Transfers and Security

The Client acknowledges and accepts that the Platform may use overseas hosting, infrastructure providers, and approved sub-processors. The Client is responsible for deciding whether this is acceptable for its business and legal obligations.

The Agency will take reasonable care in implementing the Platform and may follow the platform provider's published security guidance, but the Agency does not warrant that the Platform will be uninterrupted, error-free, immune from cyber attack, or suitable for every regulatory use case.

- The Client must enable strong passwords, user-level permissions, and multi-factor authentication wherever available.
- The Client must promptly remove access for leavers and restrict access to only those personnel who require it.
- The Client should maintain its own export and backup process for any data it considers business-critical.
- The Client must review all approved integrations and is responsible for any separate third-party terms and transfer implications triggered by those integrations.

6. Setup, Instructions and Approval

The Agency may build forms, workflows, automations, pipelines, websites, landing pages, email templates, and related assets using information supplied by the Client. The Client is responsible for checking and approving all live assets before launch, including:

- data capture fields and mandatory field logic;
- consent wording and privacy policy links;
- email and SMS content;
- automation triggers, delays, branching logic, and task assignments;
- internal user permissions and notification destinations;
- any regulated wording relevant to the Client's industry.

The Client accepts that once a workflow, form, or automation is approved or goes live, the Agency is entitled to rely on that approval unless and until the Client requests a change in writing.

7. No Legal or Regulatory Advice

Any information supplied by the Agency about privacy, consent, retention, communications law, or platform settings is provided for general operational guidance only. It is not legal advice and must not be relied upon as a substitute for advice from the Client's own solicitor or specialist adviser.

The Client must obtain independent legal advice where it is unsure about controller/processor status, lawful basis, direct marketing rules, international transfers, retention requirements, use of sensitive data, or response obligations following a personal data breach.

8. Agency Liability and Disclaimer

To the maximum extent permitted by law:

- the Agency accepts no responsibility for the Client's legal compliance, privacy notices, consent model, retention policy, record-keeping, or the lawfulness of the Client's campaigns, automations, or data processing activities;
- the Agency shall not be liable for any outage, suspension, feature change, integration failure, cyber incident, loss of data, message blocking, deliverability issue, or degradation of service arising from the Platform provider or any third-party supplier;
- the Agency shall not be liable for any indirect or consequential loss, loss of profit, loss of revenue, loss of goodwill, loss of opportunity, or regulatory fine or investigation unless caused solely and directly by the Agency's wilful misconduct;
- the Agency shall not be liable for any claim resulting from inaccurate instructions, unlawful data collection, missing notices, defective consent language, offline processes, imported lists, or content supplied or approved by the Client.

Where the law permits a financial cap rather than a total exclusion, the Agency's aggregate liability in connection with Platform-related services shall not exceed the total fees paid by the Client to the Agency for those specific services during the three months immediately preceding the event giving rise to the claim. This clause should be reviewed and amended if the Agency's main terms already contain a liability cap.

9. Client Indemnity

The Client shall indemnify and keep indemnified the Agency against all losses, damages, liabilities, costs, claims, demands, actions, penalties, fines, expenses, and professional fees arising from or connected with:

- the Client's breach of applicable data protection, privacy, marketing, consumer, or communications law;
- the Client's upload, import, capture, or use of personal data without a lawful basis or required notice/consent;
- the Client's use of restricted or sensitive data within the Platform;
- the content of any campaign, automation, landing page, message, or form approved by the Client;
- any complaint, investigation, or enforcement action resulting from the Client's instructions or business model.

10. Retention, Exports and Deletion

The Client must not assume that the Platform will automatically implement the Client's internal retention policy unless those settings have been specifically configured, tested, and documented. The Client is responsible for:

- setting an internal review cycle for stale or unnecessary data;
- deleting, suppressing, or anonymising records where legally required;
- keeping copies of any business-critical data outside the Platform where appropriate;
- making timely requests if it requires data export, transfer, deletion, or account closure support.

Following termination of services, the Agency may delete or disable access to platform assets, workflows, or data under its control after a reasonable transition period unless otherwise agreed in writing.

Schedule 1 - Platform Summary for Client Awareness

The following summary is included to help the Client understand the practical position of the underlying platform. It is provided for awareness only and may change as the platform provider updates its own documentation.

Area	Plain-English summary
Platform role	The platform provider states that it typically operates as a processor or sub-processor, while the customer may be the controller or processor depending on the customer's own business model.
Hosting location	Published materials state that product infrastructure is hosted through major cloud providers and resides in the United States.
Security controls	Published materials describe encryption in transit and at rest, access controls, logging, backups, vulnerability testing, and annual third-party penetration testing.
Payments	Published materials state that the platform should not be used to store card data directly and that payment processing is handled through PCI-compliant processors rather than by the platform itself.
Retention	Published materials indicate that customers should actively manage deletion and retention and not assume the platform alone makes them compliant.
Sub-processors	The platform provider publishes a sub-processor list and says customers may subscribe for updates to that list.

Schedule 2 - Acceptance by Use

Use of the Platform is conditional upon acceptance of these terms. No separate checklist, signature, or date-stamp process is required unless the Agency chooses to issue one.

Client Acknowledgement by Use

By asking the Agency to activate, configure, or provide access to the Platform, and by logging in to, accessing, or continuing to use the Platform, the Client confirms that it has read, understood, and agreed to these terms and the Agency's wider terms and conditions as they apply to Platform-related services. Any person using the Platform on the Client's behalf is deemed to do so with the Client's authority.