



Acceptable Use Policy

The rules for everyone who uses Precinct. Version 1.0. It forms part of your agreement with us under the Precinct Master Terms.

This policy applies to the customer named in the Order and to **everyone who uses Precinct through the customer's account**. The customer is responsible for making sure its users follow it.

1. Accounts and sign-in

- 1.1** Each user must have their **own sign-in**. Never share a sign-in, and never let anyone else use yours.
- 1.2** Protect the accounts you use to sign in to Precinct, for example your Microsoft 365 account, with a strong password and multi-factor authentication.
- 1.3** Tell us straight away at the support address if you think someone else has used your sign-in, or when a user leaves your business so that we can remove their access.

2. Text messages and emails

- 2.1** Only send messages to people you have a genuine business reason to contact, such as your own customers about their jobs, enquiries and appointments.
- 2.2 Do not use Precinct to send marketing or promotional messages** unless your Order includes a marketing feature. Where it does, you must have each person's consent where the law requires it (including under the Privacy and Electronic Communications Regulations), and you must stop messaging anyone who asks you to.
- 2.3** Never send messages that are unlawful, threatening, abusive, harassing, discriminatory, obscene, misleading or fraudulent, or that pretend to be from someone else.
- 2.4** Never send bulk or repeated messages that the recipient has not asked for, or use Precinct to collect debts in a way that breaks the law.
- 2.5 Except for automatic messages sent from templates you have approved, you must check messages before they are sent, including anything written or suggested by Precinct's AI features.** You are responsible for what you send.
- 2.6 You are responsible for approving automatic message templates before they are enabled.** Automatic messages (for example the acknowledgement sent when an email or web-form enquiry arrives) are filled-in templates, not written by AI. If a template stops being accurate, change it or tell us.

3. What you put into Precinct

- 3.1** Do not upload or store anything unlawful, anything that infringes someone else's rights, or anything containing viruses or other harmful code.
- 3.2** Do not ask your customers to send you health details, payment card details or other sensitive information through Precinct unless we have agreed it with you in writing.
- 3.3** Only keep personal data you need, and deal with requests from people about their data as the law requires. We will help you as set out in the Data Processing Agreement.

4. Security and fair use

- 4.1 Do not try to test, probe, scan or get around Precinct's security, or access any part of our systems other than through the normal Precinct pages.
- 4.2 Do not use automated tools, scripts, scrapers or AI agents to copy Precinct's screens, content or workflows, or to extract data in bulk, except through an export or connection we have provided.
- 4.3 Do not use Precinct in a way that overloads it or harms the service for others.
- 4.4 Tell us **straight away** at the support address if you notice anything that could be a security problem or a data breach.

5. What happens if this policy is broken

Depending on how serious it is, we may:

- warn you and ask you to put it right;
- **suspend** all or part of the Service, including text messages, straight away;
- **end the Agreement immediately, with costs**, under the clause "Ending the Agreement for misuse" in the Master Terms. That means the monthly fees for the rest of your contract period and our costs of dealing with the misuse become payable;
- report unlawful activity to the relevant authorities where we are required to.

Work we do to deal with a breach of this policy is chargeable at the hourly rate in your Order.

6. Changes to this policy

- 6.1 We may update this policy by giving you at least 30 days' written notice, as set out in the Master Terms.