Clearpath

PROGRAMME MANAGEMENT

ACCEPTABLE USE POLICY

Last updated: May 2026

This Acceptable Use Policy ("AUP") sets out the rules for using the Clearpath programme management platform operated by Clearpath Construction Solutions Ltd. It supplements the Terms and Conditions of Service and applies to all Customers and Authorised Users. Breach of this AUP may result in suspension or termination of access to the Service.

1. GENERAL PRINCIPLES

1.1 The Service is provided for the legitimate business purpose of construction programme management, delay tracking, site diary management, and related record-keeping. All use of the Service must be lawful, professional, and consistent with this purpose.

1.2 The Customer is responsible for the actions of all Authorised Users who access the Service using the Customer's account.

2. PERMITTED USE

2.1 You may use the Service to: (a) create, manage, and version construction programmes; (b) record activity progress, delay events, and contractual notifications; (c) maintain site diaries including workforce records, weather conditions, progress notes, and photographs; (d) upload documents, photographs, and evidence relevant to construction project management; (e) generate delay notices, reports, and exports for use in your construction projects; and (f) manage organisation membership, project access, and user permissions.

3. PROHIBITED USE

3.1 You must not use the Service to:

(a) Upload, store, or transmit any material that is unlawful, defamatory, threatening, abusive, harassing, obscene, or otherwise objectionable.

(b) Upload, store, or transmit any material that infringes the intellectual property rights, privacy rights, or other rights of any third party, including confidential documents belonging to other parties without proper authorisation.

(c) Upload photographs of identifiable individuals without a lawful basis for doing so. Where site diary photographs depict identifiable workers or visitors, the Customer is responsible for ensuring that appropriate notices have been provided to those individuals in accordance with Data Protection Law.

(d) Store or transmit special categories of personal data (as defined in the UK GDPR), including health data, trade union membership, religious or philosophical beliefs, or biometric data. The Service is not designed for this purpose and does not implement the additional safeguards required for such data.

(e) Attempt to gain unauthorised access to any part of the Service, other users' accounts, or the underlying systems and infrastructure.

(f) Use automated scripts, bots, scrapers, or similar tools to access the Service, except through the Service's own export and API functionality (if applicable).

(g) Reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the Service.

(h) Use the Service in any way that could damage, disable, overburden, or impair the Service or interfere with any other party's use of the Service.

(i) Sublicence, resell, share, or make the Service available to any third party who is not an Authorised User.

(j) Share login credentials between individuals. Each Authorised User must have their own unique account.

(k) Use the Service to send unsolicited communications, spam, or any form of marketing material to third parties.

(l) Upload or transmit any file containing viruses, malware, ransomware, or any other malicious code.

4. CONTENT STANDARDS

4.1 All content uploaded to the Service (including programme names, activity descriptions, diary entries, delay records, comments, and photographs) must: (a) be accurate and honest; (b) comply with all applicable laws; (c) not contain material that could bring the Provider into disrepute; and (d) be relevant to the legitimate business purpose of construction programme management.

4.2 The Provider does not routinely monitor content uploaded by Customers but reserves the right to review and remove content that breaches this AUP upon becoming aware of it.

5. PHOTOGRAPHS AND IMAGES

5.1 The Service allows Customers to upload photographs to site diaries and as delay evidence. When uploading photographs, Authorised Users must ensure that:

(a) Photographs do not depict illegal activity.

(b) Photographs do not contain personal data (such as identifiable faces of individuals) unless the Customer has a lawful basis for processing that data and has provided appropriate privacy notices to the individuals concerned.

(c) Photographs do not contain sensitive or classified information that should not be stored on a cloud-hosted platform.

(d) The Customer has the right to upload the photograph (i.e., it was taken by the Customer or its employees, or the Customer has permission to use it).

6. SECURITY OBLIGATIONS

6.1 Each Authorised User must: (a) choose a strong, unique password that meets the Service's minimum requirements (at least 8 characters, including uppercase, lowercase, and a number); (b) not share their password with anyone, including colleagues; (c) not use the same password that they use for other services; (d) log out of the Service when using shared or public devices; and (e) notify the Customer's organisation administrator immediately if they suspect their account has been compromised.

6.2 The Customer's organisation administrator is responsible for promptly revoking access for individuals who leave the organisation or no longer require access to the Service.

7. ENFORCEMENT

7.1 The Provider reserves the right to: (a) investigate any suspected breach of this AUP; (b) suspend or restrict access to the Service for any Authorised User or Customer that breaches this AUP; (c) remove any content that breaches this AUP; and (d) terminate the Agreement in accordance with the Terms and Conditions.

7.2 Where practicable, the Provider will give the Customer notice of a breach and a reasonable opportunity to remedy it before suspending or terminating access. However, the Provider may act immediately and without notice where the breach poses a security risk, involves unlawful activity, or could harm other customers.

8. REPORTING BREACHES

8.1 If you become aware of any breach of this AUP by another user, or if you believe the Service is being used in a manner that is unlawful or harmful, please report it to support@clearpath.build.

9. CHANGES TO THIS POLICY

9.1 The Provider may update this AUP from time to time. Material changes will be notified to Customers in accordance with the Terms and Conditions.