



Service terms

Consultancy Development AI and Client Cloud

Version 3.0 | Effective date 01/08/2026 | Disruption Works Ltd

Our agreement

These terms cover business services supplied by Disruption Works Ltd, company number 10761509, registered at 1 Davy Road, Derriford, Plymouth, England, PL6 8BX (we, us), to the client named in the order (you). This edition is effective from 01/08/2026 and applies to a client only when incorporated into an agreed order or variation. Business days are Monday to Friday excluding public holidays in England.

1 Scope and priority. The agreement comprises the accepted order, these terms, the selected service provisions and any expressly incorporated schedules. The order identifies deliverables, exclusions, assumptions, fees, timescales and responsibilities. Your purchase-order terms do not apply unless we expressly accept them. An order is accepted by signature or an express written acceptance by authorised representatives of both parties.

The processing addendum prevails for personal-data matters, subject to any mandatory transfer instrument. An expressly agreed variation identifying the affected clause takes priority; otherwise the order prevails over these terms, and the specific service provisions prevail over the general provisions. Policies and proposals are incorporated only if identified by title, version and relevant scope. An internal policy update does not itself amend this agreement.

2 Delivery and cooperation. We will provide the agreed services with reasonable skill and care, using suitably skilled personnel. We remain responsible for work we subcontract. You will provide accurate requirements, suitable access, lawful materials, timely decisions and an authorised project contact. Each party will follow reasonable security requirements notified and agreed for access to the other's systems.

Dates depend on the stated assumptions and your cooperation. If a dependency fails, we will explain the effect and propose a revised plan. Neither party is required to perform additional work without an agreed change, except for the limited emergency action permitted below. Work estimates are not fixed prices unless the order says so.

3 Changes. A change requires written agreement on scope, price, timetable and acceptance criteria. Email approval by the authorised contacts is sufficient. Meeting notes do not amend the contract unless expressly approved as a change. We may pause affected work while a material dependency or change remains unresolved, with prompt notice; unaffected work continues where reasonably practical.

GitHub Projects records delivery tasks, owners, dependencies and progress. The order identifies the agreed scope by version or retained snapshot. Authorised delivery contacts may refine work within that scope; changes to outcomes, fees, contractual dates, risk, data processing or responsibilities require the change process above. A board status, estimate, assigned task or meeting note is not by itself contractual approval, acceptance or authority to deploy. Record material decisions with the authorised approver, date and evidence, and retain the agreed record. Do not place secrets or unrestricted personal data in delivery records.

4 Fees. You will pay the agreed fees and VAT within 30 days of invoice unless the order states otherwise. The order defines deposits, milestones, subscriptions and usage charges. Expenses require prior approval. Raise genuine invoice disputes promptly with reasons and pay undisputed amounts on time. We may claim interest and recovery costs available under applicable late-payment law, without double recovery.

Our fixed fees change only by agreement. Supplier charges may be passed through only on the basis stated in the order. We will give available notice and supporting details of supplier price changes. If the parties cannot agree required adaptation or revised ongoing charges, clause 10 applies; supplier commitments remain payable only as stated there. There is no unilateral website-based price change.

Rights and information

5 Ownership. Each party keeps its existing intellectual property and materials. Unless the order expressly assigns specified bespoke deliverables on payment, we own our deliverables and grant you, on payment of the relevant fees, a perpetual, worldwide, non-exclusive, royalty-free licence to use, copy and modify the paid bespoke deliverables for the agreed business purpose, including customer-facing use and maintenance by your service providers under confidentiality obligations. This licence survives termination and does not permit standalone resale of our reusable tools.

Our pre-existing and reusable software, methods and know-how remain ours even where bespoke IP is assigned. The same licence covers such material embedded in paid bespoke deliverables to the extent needed to use them. Third-party and open-source components remain subject to their disclosed licences. AI outputs may not be unique or attract intellectual property rights; we do not promise exclusive ownership of them. Subscription platforms are licensed only for the paid subscription period. The order states what source code, configuration and documentation will be handed over. You grant us the rights in your materials needed to provide the services.

Confidentiality and responsibility

6 Confidentiality and personal data. Each party will protect the other's confidential information with reasonable care, use it only for the agreement, and disclose it only to people who need it and are bound by confidentiality, or as required by law. This does not cover information lawfully known, independently developed or public without a breach. These duties continue for five years after termination, and for trade secrets while they remain secret. Personal data remains protected for as long as it is held. Publicity, client logos and case studies require your prior written approval.

Each party will comply with data-protection law applicable to its activities. Where we process personal data on your behalf, the agreed processing addendum and completed processing schedule apply, including where data remains in your cloud. Each party is independently responsible for its own business-contact records. A privacy notice does not replace the processing addendum.

7 Liability. Nothing excludes or limits liability for death or personal injury caused by negligence, fraud, fraudulent misrepresentation, or anything that cannot lawfully be excluded or limited. No term limits rights of individuals or regulators where law prohibits this.

Subject to that protection, each party's aggregate liability under or in connection with an order, in contract, tort including negligence, breach of statutory duty or otherwise, is limited to 100% of the fee base. For breach of confidentiality or data-protection obligations the limit is 200% of the fee base. All claims combined under that order are subject to an overall 200% limit, within which ordinary claims remain subject to the 100% limit. Related claims are counted together, without double recovery.

The fee base is the fixed project fees paid or payable under the affected order plus recurring DW service fees paid or payable in the 12 months before the first event giving rise to the claim. If that event occurs in the first 12 months of recurring service, use instead the recurring fees committed for those first 12 months. VAT and separately identified pass-through supplier charges are excluded. Payment of properly due fees is not limited by this clause.

Neither party is liable for indirect or consequential loss, or loss of profit, revenue, anticipated savings or goodwill. Reasonable direct costs of restoring data or systems damaged by a party's breach are not excluded solely because they involve data loss, but remain subject to the applicable cap. Each party will take reasonable steps to reduce loss. The limitations apply only to the extent permitted by law.

8 Client and external changes. You may make changes within your rights, but must record material changes to supported systems and notify us promptly. Relevant changes include code, prompts, models, knowledge sources, permissions, tools, integrations, infrastructure, security

controls and usage outside the agreed purpose or limits. We are not responsible to the extent a failure or loss is caused by your changes, your breach or a third party outside our responsibility. This does not exclude our own contribution to a failure or our obligations for subcontracted work or personal-data processing.

We will identify the affected baseline and explain the evidence supporting an exclusion. Warranty or support relief applies only to affected functions and periods. Diagnosis, restoration, retesting and adaptation outside agreed support are chargeable at agreed rates after authorisation. If investigation establishes our breach, we bear the reasonable investigation and correction costs attributable to it. Reinstatement of a changed baseline requires agreed testing and written confirmation, not automatic cancellation of all support.

9 Suspension. We may suspend affected work or services for an immediate security, legal or material operational risk, or after seven days' written notice of undisputed overdue payment. Suspension must be proportionate, notified promptly and lifted when the reason is resolved. We will not disable client-owned cloud accounts, unrelated systems or perpetual rights in paid deliverables. Emergency containment must stay within agreed access and change authority; no destructive action or model replacement is authorised merely by this clause.

Ending the agreement

10 Duration and termination. Fixed projects run to completion unless ended under the agreement. Recurring services may be ended by either party on 30 days' written notice, effective no earlier than any minimum term expressly stated in the order. Renewals and any different notice periods must be stated in the order.

Either party may terminate an affected order for a material breach that is irremediable, or remains unremedied 30 days after written notice describing it and requiring a remedy. Either may also terminate where continued performance would be unlawful. Insolvency-related rights apply only to the extent permitted by law.

If an external provider withdraws or materially changes a required service, the parties will consider reasonable alternatives and agree their scope and cost. If no suitable solution is agreed within 30 days after notice of the material effect, either party may terminate the affected service on written notice. Immediate suspension is permitted where continued operation is unsafe or unlawful. Unaffected services continue where reasonably practical.

On termination you will pay for work properly performed and approved, unavoidable third-party commitments disclosed before commitment. We will mitigate cancellation costs. We will refund prepaid charges for services not supplied, after deducting amounts properly due; no blanket forfeiture applies. Ending a contract does not remove accrued rights, confidentiality, data obligations or paid perpetual licences.

11 Handover. We will provide the deliverables and documentation due under the order and cooperate in an orderly handover. Additional transition work is charged only at agreed rates. Your cloud tenancy and data remain under your control. We will relinquish our access as instructed after handover. Return and deletion of personal data follow the processing addendum and are not conditional on payment of a disputed invoice. We will not delete client systems or data without authorised instructions or a legal requirement.

12 Events beyond reasonable control. Neither party is liable for delay or failure caused by events beyond its reasonable control, but only to the extent affected. The affected party must notify the other promptly and take reasonable steps to reduce disruption. This does not excuse avoidable failures, payment already due, or agreed continuity obligations. After 30 days of material disruption either party may terminate the affected service, with clause 10 governing charges and refunds.

13 Notices and disputes. Formal notices must be sent to the notice email or postal address stated in the order. Email is received on the next business day after sending if no delivery failure is received; termination must not depend on our processing the email. Each party must keep contact

details current. Project leads will first seek to resolve a dispute, then refer it to senior representatives. Neither process prevents urgent court relief or statutory action. The agreement is governed by the law of England and Wales and its courts have exclusive jurisdiction.

14 General. The agreement is the entire agreement for its subject and can be varied only in writing as described above. It does not replace unrelated existing orders without express agreement. Neither party may transfer it without the other's written consent, not unreasonably withheld. No partnership or employment relationship is created. No person other than the parties may enforce it except where mandatory law or an applicable transfer instrument gives them rights. Invalid provisions are severed to the minimum necessary. Failure to exercise a right is not a waiver. Electronic signatures and counterparts are permitted.

Consultancy

A1 Advice and outputs. Consultancy covers only the workshops, analysis, recommendations and outputs in the order. Advice reflects the information supplied and circumstances at delivery. We will identify material assumptions and limitations. You remain responsible for business decisions and implementation, except for implementation services expressly allocated to us. We do not guarantee a financial result or provide regulated professional advice unless expressly agreed with appropriately qualified personnel.

A2 Reliance. Advice is for your agreed purpose and recipients. Wider distribution does not create duties to third parties. A material change in facts or intended use may require an updated assessment and agreed additional work.

Application Development

B1 Scope and dependencies. The order defines functionality, environments, integrations, deliverables, acceptance criteria and deployment responsibilities. Discovery, prototypes and production systems are distinct deliverables. A prototype is not approved for production merely because it works in a demonstration. Changes to requirements or dependencies follow clause 3.

B2 Acceptance. We will give written notice when a deliverable is ready for acceptance, with access and evidence sufficient to test it. You have 10 business days to accept it or identify material failures against the agreed criteria, with reasonable details. We will correct failures attributable to us and resubmit the affected elements for testing. Minor issues that do not materially prevent agreed use do not block acceptance and will be recorded for correction.

If you provide no response, we may issue a reminder giving a further five business days. The deliverable is then accepted if no material failure is reported and testing was reasonably possible. Deliberate production use also constitutes acceptance, except for an agreed pilot. Acceptance does not waive latent defects or other contractual rights, and does not authorise live deployment or AI actions that require separate approval.

B3 Defect correction. For 90 days after acceptance, we will correct, without additional development charge, reproducible material failures of our work to meet the agreed criteria when notified during that period. New functionality, client changes, changed data and external-provider changes are handled under clauses 3 and 8 where they cause the failure. This correction commitment does not extinguish other rights for our breach. If we cannot remedy a material failure within a reasonable time, clause 10 remains available.

B4 Maintenance and delivery. Ongoing monitoring, security maintenance, upgrades and support are included only as described in the order. The order records repository ownership, source-code access, build instructions, configuration and deployment handover. We will disclose material third-party licence constraints. We will not deploy a destructive migration without the agreed backup, validation, rollback and approval arrangements.

B5 Development and release principles. We will use the agreed repositories and conventions, supported technology, justified dependencies and documented material design decisions. We will design for maintainability and proportionate portability within scope, without promising interchangeable vendors or cost-free migration. Use named access, least privilege, MFA where supported, secrets management and appropriate environment separation. Record material dependencies and licence constraints.

Production changes require authorised human review and proportionate verification; AI review alone is insufficient. The order identifies an independent reviewer or a documented alternative. Tests and checks must reflect the risks, including security, integrations, accessibility and user acceptance as applicable. Record the tested revision, results, known limitations, target environment, release approver and post-release checks. Code review, acceptance and production approval are separate decisions; a merged change or Done issue does not prove deployment.

Material data migrations require an agreed migration or backfill method, validation, backup or recovery arrangements, rollback or restoration approach and release authority. Live data must not be reseeded, overwritten, truncated or reset as a routine deployment step. Deliberate deletion or irreversible changes require specific client authority and an appropriate recovery assessment.

B6 AI-assisted development. AI development tools may be used only for the purposes, accounts and content approved in the order, under the commercial-provider and data controls in C3, whether or not a live AI agent is commissioned. A named developer remains accountable for reviewing generated code, security and licences. Use synthetic or suitably anonymised test data by default; do not send production credentials, unrestricted production datasets or unrelated client information to AI tools. Approval of AI-assisted development does not authorise live agents or additional processing.

AI Agent Development

C1 Intended use and authority. AI services may include text, voice, retrieval, workflow automation and agents that invoke tools. The order must define permitted uses, users, data, actions, human oversight, escalation routes and operating limits. An agent may send messages, write records, make commitments, spend money or trigger physical or consequential actions only within permissions expressly approved for that purpose.

High-impact, safety-critical or regulated use, and decisions significantly affecting individuals, require a separate agreed assessment and safeguards before use. You are responsible for your deployment decisions, lawful use, end-user notices and any required consent for recording or communications. We remain responsible for implementing the safeguards allocated to us.

C2 Limits and testing. AI output is probabilistic and may be incorrect, incomplete, biased or inconsistent. We do not promise that every response will be correct or that prompt injection can always be prevented. We will nevertheless design and test the agreed safeguards with reasonable skill and care. Acceptance uses agreed representative cases, thresholds and failure handling against a recorded model and configuration; it is not a guarantee of every future output.

The baseline records model/provider identifiers, available versions, prompts, settings, knowledge sources, tool permissions and test evidence. You will approve the intended use, acceptable residual risks and live-operation authority before launch. The agreed human oversight must remain in place. Give agents only the permissions needed for approved actions; untrusted messages or retrieved content do not authorise changes to those permissions. Evaluation must include representative edge cases, unsafe inputs, tool permissions and failure handling where applicable. Material changes require proportionate reassessment and testing before the affected use resumes.

AI providers and governance

C3 Approved commercial services. Our principal AI providers are OpenAI, Anthropic, Google Gemini and Microsoft Azure OpenAI. Only the specific commercial service, contracting entity, account, deployment and settings approved in the order and processing schedule may receive client data. Naming a provider is not blanket approval of its products or of all four providers for every project. Consumer services and unapproved free tiers must not receive client confidential or personal data.

We will use commercial contractual arrangements that prohibit using client inputs, outputs, files and other client content to train or improve general-purpose or shared models, and prohibit sale or disclosure outside the authorised delivery chain. We will not enable voluntary data-sharing, feedback or model-training options. Client-specific fine-tuning is excluded unless separately authorised in writing with its purpose, data, isolation and retention controls.

Authorised processing by the provider and its approved subprocessors to deliver, secure and support the selected service is not prohibited sharing. Any abuse-monitoring retention or human review, application-state storage, legal retention, processing locations and international transfers must be documented and approved before use. A no-training commitment does not promise zero retention. Where the required restrictions cannot be met, we will not send the affected client data to that service and will propose an alternative.

C4 Provider changes and degradation. Providers control their models and may change behaviour, capacity, latency, pricing, interfaces, safety filters, terms, versions or availability. We cannot guarantee a model's continued availability or identical future behaviour. Clause 8 applies to failures caused by changes outside our control; it does not excuse our failure to implement agreed resilience or change-management duties.

We will notify you promptly when we become aware of a material impact on your service and propose proportionate mitigation. Continuous provider monitoring applies only if included in the order. Retesting, migration and adaptation are included only to the extent stated in the order or needed to remedy our own breach; other work requires an agreed change. We will not silently switch provider, enable training or materially change data locations, retention or permissions. If privacy restrictions cease to be met, affected processing must pause pending an approved compliant solution. Clause 10 provides an exit where an alternative cannot be agreed.

C5 Client changes and support. Client access does not transfer responsibility for every failure to the client. However, changing prompts, knowledge, tools, models, safety settings or permissions may invalidate earlier test results for affected behaviour. You will retain change records, notify us of material changes and obtain review where required by the agreed operating controls. Investigation, retesting and restoration follow clause 8. Support targets may be paused only for the affected work while necessary access, evidence or a supported configuration is unavailable, with reasons and next steps communicated to you.

C6 AI management approach. We are developing our AI governance approach with reference to ISO/IEC 42001. We do not represent that we are certified to, or currently fully conform with, that standard. For the project we will carry out the specific risk assessment, documentation, testing, human-oversight, change-control and incident-management activities allocated to us in the order. This is not a guarantee of certification, regulatory approval or risk-free AI.

Each party will report material AI safety, security or performance incidents promptly to the agreed contacts, preserve relevant evidence lawfully, and cooperate on containment and corrective action. The order identifies who can disable agent actions, approve restart and review residual risk. Personal-data incidents also follow the processing addendum. Ongoing evaluation and review frequencies must be expressly scoped.

Client Cloud Deployment and Support

D1 Default operating model. We deploy into your cloud account unless the order expressly states otherwise. You contract with and pay the cloud provider directly, own the tenancy and retain administrator control. Our service is the agreed design, configuration, deployment or management work; we do not sell an underlying cloud availability guarantee merely by deploying an application.

D2 Shared responsibilities. The order allocates responsibility for identity and access, network configuration, application security, patching, backups, restore testing, monitoring, incident response, capacity, budgets and disaster recovery. By default, you manage the tenancy, billing, tenant-wide identity and security policies, and ongoing operations after handover. We manage the configuration and deployment work expressly allocated to us and protect our access and credentials. The cloud provider manages its own infrastructure under your provider contract.

We will document material handover requirements and known limitations. An unallocated operating duty does not silently become a managed service. Before production release, the order must identify owners for backups, security maintenance and incident response. We remain responsible for exercising reasonable skill and care in our own work, including any delegated tenant-level work.

D3 Access and changes. You will provide named, least-privilege access adequate for our agreed tasks and maintain authorised access while those tasks are required. We will use that access only for authorised purposes and follow agreed controls. Both parties must record material production changes. If access is removed or the environment is changed, we will explain the effect on delivery or support. Relief and additional charges are limited to the affected work under clause 8.

D4 Resilience and costs. Backup ownership, retention, restore testing and any recovery objectives must be stated in the order. No recovery time or recovery point is guaranteed unless expressly agreed. Before a material deployment, the parties will implement the agreed backup and rollback arrangements. You remain responsible for cloud and AI usage billed to your accounts, but this does not exclude our liability for excess costs caused by our breach. Budget alerts are not spending caps unless explicitly implemented and tested as such.

D5 Support levels. Support hours, severity definitions, response targets, monitoring coverage, exclusions and any service credits are as stated in the order. Response targets are not guaranteed resolution times. We will cooperate with provider incident handling within the agreed support scope. Provider credits are governed by the relevant provider contract; there is no automatic matching DW uptime promise.

D6 Other hosting models. DW-hosted, reseller, shared-platform or fully managed hosting requires an express additional schedule addressing billing, infrastructure control, security, service levels and exit. These client-cloud defaults must not be reused for a different hosting model without that schedule.