Business Continuity Plan

DOCUMENT MOG-BCP-001 | REV 0 | 16 OCTOBER 2026 | APPROVED

Mogas Design Limited • Company No. 15188968 • 5th Floor, 167–169 Great Portland Street, London, W1W 5PF (correspondence address only)

1. Purpose and scope

This plan sets out how Mogas Design Limited maintains essential consultancy services and recovers from interruption affecting engineering design, technical reviews, independent approvals/appraisals, document access, communication, equipment, site visits or contractor availability.

2. Organisation and critical operations

Mogas is a remote husband-and-wife business with two directors (60%/40% share ownership) and no salaried employees. Its principal working area is a converted garden office at a director's residence; the London address is correspondence-only, not a staffed office. Independent self-employed or limited-company subcontractors ordinarily work from their own locations. Critical operations are client communications, access to current design inputs, engineering production/checking, approved deliverables, project records and invoicing.

3. Responsible persons and activation

The managing/project director coordinates continuity response and records incidents and decisions; the second director supports client updates and business administration as appropriate to availability and authority. Activate this plan when a disruption threatens safety, data access, delivery, legal compliance, contract requirements or customer deadlines. Preserve safety first, then assess service impact, notify affected clients where appropriate and allocate recovery actions.

4. Cloud files, access and backup arrangements

Mogas uses online drive/cloud file storage for its working project documents and business records. Authorised directors can access their accounts from another trusted or replacement device by securely signing in, allowing remote recovery if the normal office computer fails or the garden office is inaccessible. Cloud synchronisation is not necessarily an independent backup. The director must verify whether version history, deleted-file recovery and a separate backup are enabled; confirm backup frequency, account recovery options and perform a documented restore test. Do not claim an unverified backup system as operational.

5. Device and account recovery

- If a laptop or computer fails, use an alternative trusted device and secure network; access the company email and document accounts using approved credentials and multi-factor authentication.
- Maintain at least two secure recovery methods, including backup/recovery codes stored separately and appropriately protected. Never share passwords or MFA codes with contractors.
- If equipment is stolen or an account appears compromised, revoke sessions, rotate credentials, secure data and assess UK GDPR or customer contractual notification duties.
- Test access to essential accounts and recovery of sample files at least annually and record results.

6. Alternate workplace and communications

Where the garden office is unavailable (fire, electrical fault, extreme weather or access issue), directors can work from another suitable safe location with secure internet and equipment. If home internet fails, use an approved alternative connection or agreed temporary location. Inform customers of changed arrangements and use email/mobile contact as available. Preserve confidentiality and avoid handling sensitive project files over insecure shared devices or networks.

7. Alternative engineering resource capacity

Mogas maintains a list of engineers and specialist subcontractors who may be able to mobilise at short notice. The resourcing approach is not dependent on a single individual: normally two or three candidate engineers are identified for each relevant discipline (e.g. mechanical, civil, stress/piping and hazardous areas, as applicable to the appointment). The director checks actual availability, current competence, required approvals/appraiser registrations, independence, insurance, conflict-of-interest position and client acceptance before substitution. No guarantee is made that all candidates are available simultaneously.

8. Handover and document control

For a key-person absence, identify outstanding tasks, deadlines, latest controlled drawings/calculations, client instructions, review registers and unclosed safety-critical issues. Transfer the work securely to a suitably competent alternative with a written handover. Only authorised persons may issue formal independent approvals/appraisals. Record substitute appointment, technical checks, revision status and communication to the client.

9. Disruption scenarios and response

- Illness/unavailability: redistribute urgent work to an available qualified engineer; notify clients about material changes to delivery dates.
- Loss of computer or data: secure accounts, recover from cloud and verified backup, test integrity and review access rights.
- Power/internet outage: switch to alternative safe device/connection or location; prioritise time-critical communications.
- Cyber incident: stop compromised access, preserve evidence, change credentials, seek IT assistance and assess data breach responsibilities.
- Inaccessible office/fire/flood: protect people, contact emergency services if required and work remotely from a safe alternate location.
- Client gas-site incident: follow site operator emergency arrangements and pause affected activities pending authorisation to resume.

10. Prioritisation and recovery objectives

Priority 1: immediate safety, data security and urgent client communications. Priority 2: retrieve controlled project information and restore essential email/files. Priority 3: assign competent resources and resume safety-critical deliverables. Recovery time and recovery point targets shall be set for each critical system following verification of actual account, storage and backup capability; no unsupported fixed restoration time is promised.

11. Records, testing and review

Maintain a current engineer-resourcing list (confidential), key client contact register, critical software/account inventory, backup and restore-test record, and interruption log with corrective actions. Check contact and resourcing details at least annually and after significant change. Run a tabletop continuity exercise annually; record any weaknesses and close actions.

12. Verification required before claiming implementation

- Confirm the actual cloud storage service(s), retention, version-history and backup method/frequency.
- Document a successful sample restore and alternative-device access test without recording credentials in the register.
- Confirm named authorised account administrators and secure recovery arrangements.
- Maintain a dated, current two-to-three-engineer shortlist for each discipline and verify willingness and availability periodically.
- Confirm client contracts permit proposed subcontracting, substitutions and remote processing.

Document control and director approval

Document number	**MOG-BCP-001**
Version	Rev 0
Document review date	16 October 2026
Next scheduled review	16 October 2027 (or sooner following significant change)
Director	Mohammed Fasiuddin
Status	Approved by the Director

Director signature:

Signed copy held on file – available on request.

Code of Conduct

DOCUMENT MOG-POL-COC-001 | REV 0 | 16 OCTOBER 2026 | APPROVED

Mogas Design Limited • Company No. 15188968 • 5th Floor, 167–169 Great Portland Street, London, W1W 5PF (correspondence address only)

1. Purpose and application

This Code of Conduct defines the standards expected of both directors and all independent contractors providing services on behalf of Mogas Design Limited. Independent contractors are not represented as employees; applicable engagement terms and statutory obligations remain in force.

2. Professional integrity and legal compliance

- Act honestly, fairly and professionally in all client, supplier and contractor interactions.
- Comply with applicable laws, client policies and project specifications; do not falsify qualifications, experience, timesheets, expenses or records.
- Make technical judgements objectively, record limitations and escalate significant safety, quality and compliance concerns.
- Only undertake work within appropriate competence, registration and formal approval authority.

3. Safety, environment and fitness for work

- Follow Mogas risk assessments and applicable client/site-specific controls, inductions and permits.
- Stop or withdraw from unsafe work and report hazards, accidents and near misses without delay.
- Remain fit for duty; do not work impaired by alcohol, illicit drugs, fatigue or other conditions affecting safe performance.
- Minimise unnecessary travel, waste and environmental impacts and promptly report environmental incidents.

4. Respect and equal treatment

Treat colleagues, clients, suppliers and the public respectfully. Bullying, harassment, discrimination, intimidation or abusive conduct are unacceptable, including in digital communications and when on client sites.

5. Conflicts of interest, gifts and anti-bribery

Disclose financial, personal or commercial conflicts which could affect impartiality. Do not give, request or accept bribes or improper incentives. Gifts and hospitality must be modest, lawful, transparent and compliant with the client's requirements; report any concern to a director. Approver/appraiser independence rules take precedence where stricter.

6. Confidentiality, privacy and information security

- Keep customer and company information confidential and use it only for authorised purposes.
- Use approved company document systems and secure access controls; maintain strong passwords and multi-factor authentication.
- Never share account credentials; report suspected loss, theft, data breaches or unauthorised access immediately.
- Do not disclose client materials to another engineer or external party without appropriate permissions and contractual safeguards.
- Observe applicable UK GDPR/data-protection obligations and confidentiality clauses.

7. Deliverables and client communication

Communicate factually and courteously; distinguish confirmed facts from assumptions and unresolved matters. Observe agreed scope, controlled revisions, dates and review/approval workflows. Report potential non-conformances, delays or mistakes quickly; do not quietly alter issued design records.

8. Contractor conduct and representation

Each contractor operates under their own contractual and tax status. Contractors must not claim to be authorised directors, employees, technical approvers or client representatives unless expressly appointed. Subcontract further only with prior authorisation and subject to confidentiality, client and competence requirements.

9. Raising concerns and breaches

Concerns should be reported promptly to either director, including suspected conflicts, bribery, bullying, unsafe practice, information leaks and inaccurate engineering records. Reports will be assessed proportionately and sensitively; retaliation against a person raising a genuine concern is not acceptable. Serious breaches may lead to withdrawal of assignments or contractual action.

10. Communication and annual review

Provide this Code to relevant contractors before appointment or on onboarding; retain acknowledgement in the contractor file. Review at least annually and after relevant regulatory, contractual or organisational changes.

Document control and director approval

Document number	**MOG-POL-COC-001**
Version	Rev 0
Document review date	16 October 2026
Next scheduled review	16 October 2027 (or sooner following significant change)
Director	Mohammed Fasiuddin
Status	Approved by the Director

Director signature:

Signed copy held on file – available on request.