

HappyIoT – G-Cloud SaaS Terms & Conditions

1. Definitions

1.1 “**Agreement**” means these Terms & Conditions, the Call-Off Contract, the Order Form, the Data Processing Addendum (Annex C), and any incorporated documents.

1.2 “**Customer**” means the contracting public sector body procuring the Service through G-Cloud.

1.3 “**Service**” or “**HappyIoT**” means the multi-tenant, browser-accessible SaaS platform for IoT telemetry ingestion, monitoring, rules-based automation, analytics and reporting, as described in Section 4.

1.4 “**User**” means an individual authorised by the Customer to access the Service.

1.5 “**Customer Content**” means data uploaded to or collected by the Service on the Customer’s behalf, including environmental telemetry, device health, automation and audit logs, and (where enabled) CCTV metadata/images.

1.6 “**SLA**” means the service level targets and credits in **Annex A**.

1.7 “**Support**” means the service management and helpdesk described in **Annex B**.

2. Structure & Precedence

2.1 The Agreement comprises (in order of precedence): (a) the G-Cloud Call-Off Contract; (b) the Order Form; (c) these T&Cs; (d) Annexes A–D; and (e) any other incorporated documents.

2.2 Conflicts are resolved by the order above.

3. Scope (SaaS-Only)

3.1 The Service provided under this Agreement is **SaaS only**. No hardware, installation, on-site survey, or physical works are included.

3.2 Hardware and on-site services may be obtained via separate, non-G-Cloud arrangements and are not part of this Call-Off.

4. Service Description

4.1 HappyIoT provides:

- (a) **Device and estate management** (software on-boarding, grouping, lifecycle states);
- (b) **Telemetry ingestion & monitoring** for environmental/safety data (e.g., temperature, humidity, CO₂, VOCs, movement/vibration and other supported metrics);
- (c) **Rules, alerts & automation** (thresholds, notifications, workflow triggers);
- (d) **Dashboards, analytics & reporting**, including compliance and wellbeing indicators;
- (e) **APIs & integrations** with approved third-party systems;
- (f) **Audit logging and security features** (e.g., MFA).

4.2 The platform supports regulatory use-cases (e.g., damp & mould risk modelling using dew-point, HHSRS-linked indicators) but is a **decision-support** tool and **does not itself assure compliance**.

5. Access & Licensing

5.1 Social Telecoms grants the Customer a non-exclusive, non-transferable right for Users to access the Service during the Term, subject to this Agreement.

5.2 User accounts are personal; credential sharing is prohibited.

5.3 The Customer is responsible for all activities under its tenant and Users' accounts.

6. Customer Responsibilities

6.1 Maintain up-to-date User records, assign appropriate roles, and enable MFA where mandated.

6.2 Ensure devices and networks under Customer control can transmit data to the platform (power/connectivity are Customer responsibilities).

6.3 Configure and maintain rules/alerts and **act on alerts** in a timely manner.

6.4 Obtain necessary resident/third-party notices and consents for data capture (including environmental and CCTV data, where enabled).

6.5 Do not rely on the Service as a life-critical system or as a substitute for statutory inspections.

7. Supplier Responsibilities

7.1 Provide the Service substantially in accordance with Section 4 and **Annex A**.

7.2 Operate, secure and maintain the cloud platform, including patches and updates.

7.3 Provide Support per **Annex B**.

8. Security

8.1 Social Telecoms implements appropriate technical and organisational measures, including encrypted transport (TLS), role-based access control, MFA support and audit logging.

8.2 The Customer must notify Social Telecoms without undue delay of any suspected unauthorised access to the tenant or User accounts.

9. Data Protection

9.1 **Roles.** The Customer is **Controller** and Social Telecoms is **Processor** in respect of Customer Content.

9.2 **Processing.** Details of processing, categories of data subjects/data and retention are set out in **Annex C (DPA)**. Environmental telemetry, device diagnostics, motion/vibration data, automation/audit logs and optional CCTV metadata/images may be processed.

9.3 **Locations & Sub-processors.** Processing locations (UK/EU) and sub-processors will be listed in Annex C and may be updated per DPA change process.

9.4 Each party shall comply with UK GDPR and the Data Protection Act 2018.

10. Acceptable Use

10.1 The Customer shall not: (a) use the Service unlawfully; (b) attempt to circumvent security; (c) introduce malware; (d) use captured media (e.g., CCTV) in breach of law or without appropriate notices/consents.

10.2 Social Telecoms may suspend access for security, legal or material-breach reasons.

11. Integrations & APIs

11.1 APIs and third-party integrations are provided on a reasonable-efforts basis and may be subject to vendor limits or change. The platform is device/brand-agnostic at the software layer, but compatibility is not guaranteed for every device.

11.2 Customer remains responsible for any third-party licences.

12. Service Levels; Maintenance

12.1 Service levels and credits are set out in **Annex A**.

12.2 Planned maintenance will be notified in advance; emergency maintenance may occur when required to protect the Service.

13. Warranties

13.1 Each party warrants that it has authority to enter into this Agreement.

13.2 Social Telecoms warrants that the Service will be provided with reasonable skill and care.

13.3 The Service is provided “as-a-service”; uninterrupted or error-free operation is not guaranteed.

14. Indemnities

14.1 Social Telecoms shall indemnify the Customer against third-party claims alleging that the Service (as provided by Social Telecoms) infringes UK intellectual property rights, subject to customary exclusions and Customer’s prompt notice/co-operation.

14.2 The Customer shall indemnify Social Telecoms against claims arising from Customer Content or misuse of the Service.

15. Liability

15.1 Neither party excludes liability for death/personal injury caused by negligence, fraud, or any liability that cannot be excluded by law.

15.2 Subject to 15.1, neither party is liable for indirect/consequential loss (including loss of profits, revenue, savings, goodwill or data).

15.3 Subject to 15.1 and 15.2, each party's aggregate liability in any Contract Year shall not exceed the total Charges paid/payable for the Service in that Contract Year.

16. Charges & Payment

16.1 Charges are subscription-based as set out in the Order Form and the associated G-Cloud pricing.

16.2 Invoices are payable per the Call-Off and Order Form. No advance hardware or installation fees apply under this SaaS Call-Off.

17. Term, Renewal & Termination

17.1 The Term is defined in the Order Form.

17.2 Unless prohibited by the Framework, the Service may renew in accordance with the Call-Off terms.

17.3 Either party may terminate for material breach not remedied within 30 days' notice, insolvency, or as otherwise permitted by the Call-Off.

17.4 For convenience termination (where allowed by the Call-Off), Customer will pay accrued Charges to the effective termination date.

18. Exit & Data Portability

18.1 On termination/expiry, Customer may export Customer Content via CSV/JSON or APIs within 30 days of termination (or as agreed).

18.2 Social Telecoms will delete or return Customer Content per **Annex C (DPA)** and documented retention settings.

18.3 Off-boarding assistance may be provided via Lot 3 (Cloud Support) under a separate Call-Off, if requested.

19. Out-of-Scope Services (for Clarity)

19.1 Device hardware; on-site surveys; installation; cabling/network changes; physical maintenance; resident engagement/training relating to physical devices; and retrofits are not supplied under this SaaS Call-Off.

20. Governing Law & Jurisdiction

20.1 England and Wales law governs; the courts of England and Wales have exclusive jurisdiction.

Annex A – Service Levels (SaaS)

A1. Availability. Platform availability target: **99.9%** per calendar month, excluding Planned Maintenance and force majeure.

A2. Telemetry Ingestion. Where supported devices are online and connected, the Service targets real-time or near-real-time ingestion; performance may vary by device vendor/network conditions (not guaranteed).

A3. Maintenance. Planned maintenance notified ≥ 72 hours in advance; emergency maintenance as required for security/stability.

A4. Exclusions. Customer networks, device power/connectivity, third-party device faults, or events outside Social Telecoms' reasonable control.

Annex B – Support & Service Management

B1. Hours. Standard Support: 09:00–17:00 UK time, Monday–Friday (excl. UK public holidays).

B2. Channels. Web portal/email/phone ticketing; incident tracking and updates.

B3. Severity & Response Targets.

- **P1 – Critical outage (platform-wide):** response 1 business hour; work continuously until workaround/restoration.
- **P2 – Major degradation (significant tenant impact):** response 2 business hours.
- **P3 – Minor degradation / functional issue:** response 8 business hours.
- **P4 – How-to / request / cosmetic:** response 2 business days.

B4. Changes. Standard changes scheduled within business hours; emergency changes executed under change control.

Annex C – Data Processing Addendum (Article 28 UK GDPR)

C1. Subject-Matter & Duration. Provision of the HappyIoT SaaS during the Term.

C2. Nature & Purpose. Collection, storage, analysis and presentation of IoT telemetry and related artefacts to support housing compliance, wellbeing and operations.

C3. Categories of Data. Environmental telemetry (temperature, humidity, CO₂, VOCs), device diagnostics/health, motion/vibration signals, automation rules/logs, audit logs; optional CCTV metadata/images where enabled.

C4. Categories of Data Subjects. Residents/occupants (indirect environmental readings), Customer staff/admin users, contractors (where user accounts are provisioned).

C5. Processing Locations. UK and/or EU data centres (as stated in the Order Form).

C6. Security Measures. TLS in transit; role-based access; MFA; audit logging; tenant segregation.

C7. Retention & Deletion. Default telemetry retention 12 months; configurable extensions by agreement; deletion/export upon termination per Section 18.

C8. Sub-processors. A current list and notice mechanism will be maintained; Customer may object on reasonable grounds as set out in the DPA.

C9. Assistance. Social Telecoms will assist with data subject requests, incident notifications and DPIA cooperation in line with statutory obligations.

C10. Audit. On reasonable notice, Customer may audit compliance once per year (or following a material incident), subject to confidentiality and platform security requirements.

Annex D – G-Cloud Service Definition Alignment

This section aligns key T&Cs content to the CCS **Service Definition** headings for SaaS listings.

D1. Service Summary (What the service does; who will use it).

HappyIoT is a housing-focused, device-agnostic IoT SaaS platform providing telemetry ingestion, monitoring, automation and reporting for compliance and wellbeing use-cases. Typical users include Compliance, Asset, Repairs and Housing teams.

D2. Benefits.

Earlier hazard detection (e.g., damp/mould risk), improved insight via consolidated dashboards, faster response through rules-based alerts, and better auditability for compliance reporting.

D3. Onboarding.

Tenant creation, user provisioning, SSO/MFA setup, API keys, and device registration (software onboarding). Any physical work is out of scope for G-Cloud.

D4. Offboarding.

Data export (CSV/JSON/APIs), tenant closure, optional assistance under Lot 3 (Cloud Support).

D5. Pricing.

Subscription pricing per tenant/users/devices or data volume, as set out in the G-Cloud pricing document; no hardware or installation charges under this Call-Off.

D6. Service Constraints.

Performance depends on third-party devices, connectivity and power; not life-critical; not a substitute for statutory inspections; integrations subject to third-party change.

D7. Service Levels.

Availability target 99.9% (Annex A); incident response targets (Annex B).

D8. Support.

Standard business-hours Support; severity-based responses (Annex B).

D9. Security.

TLS in transit, RBAC, MFA, audit logging, tenant isolation.

D10. Data Location / Sovereignty.

UK/EU as defined on Order Form; DPA in Annex C.

D11. Identity & Access Management.

Named users, roles/permissions, SSO/MFA supported.

D12. Backup/Restore & DR.

Provider-managed backups; recovery objectives designed for platform resilience; details available on request under NDA.

D13. Accessibility.

Browser-based UI designed to align with GOV.UK accessibility guidance; specific statements available on request.

D14. Roadmap (Non-Binding).

Platform enhancements may include expanded device integrations and analytics features; roadmap items are not contractual.

End of Document