

STAT SOLUTIONS LTD (T/A ASSET FOR VIRTUAL SCHOOLS)

GENERAL TERMS AND CONDITIONS OF CONTRACT (G-CLOUD / PUBLIC SECTOR)

1. Definitions and Interpretation

1.1 Definitions

“Acceptable Use Policy” means the rules for use set out in Schedule 6.

“Approval” means written approval by the Authority’s Contract Manager.

“Authority Data” means all data (including Personal Data) provided by/on behalf of the Authority, or created/processed in providing the Services.

“Authorised Users” means users permitted by the Authority to access ASSET.

“Business Day” means Monday to Friday (excluding public holidays in England).

“Change” means any addition, removal or variation to the Services, SLA, Charges, implementation approach, or deliverables.

“Change Control Procedure” means the procedure in Clause 12 and Schedule 7.

“Charges” means the fees payable under Schedule 2 and the Order Form.

“Confidential Information” means information disclosed by a Party that is confidential by nature or marked confidential, including Authority Data.

“Contract” means the Order Form, these Terms, and all Schedules (and any signed Change Notes).

“Contract Manager” means each Party’s named contract manager in the Order Form (or replacement notified in writing).

“Contract Term” means the period in the Order Form (1–3 years), including any agreed extension.

“Data Protection Legislation” means the UK GDPR, Data Protection Act 2018, PECR where applicable, and ICO guidance/codes where relevant.

“DPA” means the Data Processing Addendum in Schedule 4.

“Exit Services” means offboarding support and data return described in Schedule 5.

“FOIA” means the Freedom of Information Act 2000.

“EIR” means the Environmental Information Regulations 2004.

“Implementation Services” means onboarding/configuration/training/migration as set out in Schedule 1.

“Order Form” means the document signed by both Parties setting out the commercial terms.

“Personal Data” has the meaning in Data Protection Legislation.

“SLA” means service levels and support provisions in Schedule 3.

“Services” means the services described in Schedule 1, including ASSET platform access and agreed modules (ePEP, attendance monitoring, analytics, reporting, support).

“Sub-processor” means any third party appointed by the Service Provider to

process Personal Data on behalf of the Authority under the DPA.

“Term” means the Contract Term.

1.2 Interpretation

Headings do not affect meaning. “Including” means “including without limitation”.

References to legislation include amendments/replacements.

2. Contract Structure and Priority

2.1 Documents forming the Contract

The Contract consists of:

- Order Form
- These Terms
- Schedule 1 (Service Specification)
- Schedule 2 (Charges & Payment)
- Schedule 3 (SLA & Support)
- Schedule 4 (Data Processing Addendum)
- Schedule 5 (Exit & Data Return)
- Schedule 6 (Acceptable Use & Safeguarding)
- Schedule 7 (Change Control)
- Schedule 8 (Security Measures / TOMs Summary)
- Schedule 9 (FOIA/EIR Support Protocol)

2.2 Order of precedence

If there is conflict: **Order Form → Change Note → Schedule 1 → Schedule 3 → Schedule 4 → remaining Schedules → these Terms.**

Authority purchase order terms do not apply unless expressly agreed in writing.

3. Commencement and Term

3.1 Commencement

The Contract starts on the Effective Date in the Order Form.

3.2 Term

The Term is **1–3 years** as stated in the Order Form.

3.3 Extensions

Any extension must be agreed in writing before expiry and may include a Charges review in line with Schedule 2.

4. Provision of Services

4.1 Service Provider obligations

The Service Provider shall:

1. provide the Services in accordance with Schedule 1 and the SLA;
2. use reasonable skill and care and good industry practice;
3. comply with applicable law;
4. maintain suitably trained staff;
5. cooperate with the Authority reasonably in relation to service reviews, audits, FOIA support, and safeguarding requirements.

4.2 Authority obligations

The Authority shall:

1. provide timely access to required data, systems, contacts and decisions;
2. ensure Authorised Users comply with Schedule 6;
3. ensure it has lawful basis/authority to provide Authority Data to the Service Provider;
4. promptly notify the Service Provider of suspected credential compromise or data incidents affecting the Services.

4.3 Dependencies and assumptions

Any key assumptions (e.g., data formats, MIS extracts, access arrangements) are listed in Schedule 1. If those assumptions change, the Parties will use Change Control.

5. Governance, Reporting and Meetings

5.1 Contract management

Each Party will appoint a Contract Manager.

5.2 Meetings and reporting

The Service Provider will provide reporting as per Schedule 3 and participate in contract review meetings as agreed (typically monthly/quarterly).

5.3 Escalation

Escalation routes and timescales are set out in Schedule 3.

6. Staff, Safeguarding and Conduct

6.1 Staff suitability and training

The Service Provider will ensure Staff are competent and appropriately trained.

6.2 Safeguarding

Where Services interact with children, schools, or sensitive pupil records:

- the Service Provider will maintain safeguarding policies and escalation procedures (Schedule 6);
- where on-site work is agreed, the Service Provider will comply with site safeguarding rules, including sign-in/out and visitor protocols.

6.3 Replacement of Staff

The Authority may request replacement of any Staff member whose conduct or performance is reasonably considered unsuitable.

7. Charges, Invoicing and Payment

7.1 Charges

Charges are as per Schedule 2 and the Order Form.

7.2 Invoicing and payment terms

Invoices will be issued as set out in the Order Form. Payment is due **30 days** from receipt of a valid invoice unless stated otherwise in the Order Form.

7.3 Disputed invoices

Disputes must be notified within **10 Business Days** with reasons. The Authority will pay undisputed amounts on time.

7.4 Taxes

VAT is payable where applicable.

8. Confidentiality

8.1 Confidentiality obligations

Each Party will:

- keep the other's Confidential Information confidential;
- use it only to perform the Contract;
- restrict access to those who need to know and are bound by confidentiality.

8.2 Permitted disclosures

Confidential Information may be disclosed where required by law (including FOIA/EIR), court order, regulator, auditors, or professional advisers.

8.3 Duration

Confidentiality survives termination for **6 years** (or longer where required by law).

9. Data Protection

9.1 Roles

Unless the Order Form states otherwise:

- Authority is **Controller**
- Service Provider is **Processor**

9.2 Data Processing Addendum

The Parties agree Schedule 4 (DPA), which forms part of this Contract.

10. Information Security

10.1 Security measures

The Service Provider will maintain appropriate technical and organisational measures (TOMs) as set out in Schedule 8.

10.2 Security incidents

The Service Provider will notify the Authority without undue delay after becoming aware of a Personal Data Breach, in accordance with Schedule 4.

10.3 Audit support (security)

On reasonable notice, the Service Provider will provide:

- relevant policies/certificates (where held),
 - pen test summaries (where available and appropriate),
 - security assurance responses consistent with public sector expectations, subject to confidentiality and security restrictions.
-

11. FOIA and EIR

The Parties will comply with Schedule 9 (FOIA/EIR Support Protocol). The Authority remains the decision-maker on disclosures.

12. Change Control

Any Change must follow Schedule 7. No Change is effective unless signed by both Parties.

13. Subcontracting and Sub-processors

13.1 No subcontracting without approval

The Service Provider will not subcontract material performance of the Services without Authority Approval, except pre-approved subcontractors listed in Schedule 4 and/or the Order Form.

13.2 Sub-processors

Sub-processors (for Personal Data processing) are governed by Schedule 4. The Service Provider remains liable for Sub-processor performance.

14. Intellectual Property Rights

14.1 Background IPR

Each Party retains ownership of its Background IPR.

14.2 Licence to use the Services

The Service Provider grants the Authority a non-exclusive, non-transferable licence for Authorised Users to access and use ASSET during the Term for internal Authority purposes.

14.3 Authority Data

Authority retains all rights in Authority Data. The Service Provider may use Authority Data only to provide and improve the Services for the Authority and as permitted by the DPA.

14.4 Feedback

If the Authority provides feedback, the Service Provider may use it to improve ASSET, provided no Personal Data is used outside the Contract scope.

15. Warranties

15.1 Service warranty

The Service Provider warrants that it will provide the Services with reasonable skill and care.

15.2 Platform conformity

The Service Provider warrants ASSET will materially conform to Schedule 1 during the Term.

15.3 Exclusions

The Service Provider is not responsible for failures caused by:

- Authority systems or third-party systems outside Service Provider control;
- misuse by Authorised Users;
- unsupported integrations not listed in Schedule 1;
- Force Majeure (Clause 21).

16. Remedies and Service Credits

16.1 SLA remedies

Where SLA failures occur, remedies (including any service credits, if selected) are set out in Schedule 3.

16.2 Rectification

The Service Provider will use reasonable efforts to rectify service issues promptly in line with severity.

16.3 Step-in / alternative provision (serious failure)

If there is persistent material failure and the Service Provider does not remedy within agreed timeframes, the Authority may procure temporary replacement services and recover reasonable incremental costs attributable to the Service Provider's breach (subject to mitigation and evidence).

17. Liability and Indemnities

17.1 Unlimited liabilities

Nothing limits liability for:

- death or personal injury caused by negligence;
- fraud or fraudulent misrepresentation;
- any liability that cannot be limited by law.

17.2 Liability cap (your requirement)

Subject to Clause 17.1, each Party's total aggregate liability in any rolling 12-month period is capped at **100% of Fees paid or payable** under this Contract in that same 12-month period.

17.3 Excluded losses

Subject to Clause 17.1, neither Party is liable for:

- indirect or consequential loss;
- loss of profit, revenue, goodwill, or anticipated savings, except where such losses are recoverable under law and cannot be excluded.

17.4 IP infringement indemnity

The Service Provider will indemnify the Authority against third-party claims that ASSET infringes UK IPR, provided that the Authority:

- promptly notifies the Service Provider;
 - allows the Service Provider to control the defence/settlement;
 - provides reasonable assistance.
- If infringement is confirmed, the Service Provider will, at its option: procure continued use, replace/modify to be non-infringing, or terminate the affected Services with a pro-rata refund of prepaid unused Fees for that affected part.

17.5 Data / content indemnity (Authority)

The Authority indemnifies the Service Provider against third-party claims arising from Authority Data supplied by the Authority that infringes rights or is unlawful, except to the extent caused by the Service Provider's breach of the DPA or misuse.

18. Termination

18.1 Termination for cause

Either Party may terminate with immediate effect by written notice if the other Party:

- commits a material breach that is not capable of remedy; or
- commits a material breach capable of remedy and fails to remedy within **30 days** of notice requiring remedy; or
- becomes insolvent, enters administration, or is unable to pay debts as they fall due.

18.2 Authority termination for safeguarding/security emergency

Where the Authority reasonably believes continued provision would create immediate risk to children, schools, or security, it may suspend or terminate the relevant element immediately, with prompt follow-up explanation.

18.3 Suspension

The Service Provider may suspend access where required to protect security, data, or service integrity, and will notify the Authority as soon as reasonably practicable.

18.4 Termination for convenience (your requirement)

Either Party may terminate for convenience on **30 days' written notice**.

18.5 Effects of termination

On termination/expiry:

- fees due up to termination are payable;
- Exit Services apply (Schedule 5);
- confidentiality and data protection obligations continue;
- licences end after the Exit Period, except as needed for data return.

19. Exit, Data Return and Retention (6 months)

Exit obligations are governed by Schedule 5. **Authority Data will be retained for 6 months** after termination/expiry (unless the Authority instructs earlier deletion), subject to legal retention and backup rotation.

20. Audit, Records and Transparency

20.1 Records

The Service Provider will maintain accurate records relating to performance, security incidents, changes, and support as appropriate for a public sector contract.

20.2 Audit cooperation

On reasonable notice, the Service Provider will cooperate with Authority audit requests proportionately, subject to confidentiality and security constraints.

21. Force Majeure

Neither Party is liable for failure caused by events beyond reasonable control. If a Force Majeure event continues for **60 days**, either Party may terminate on written notice.

22. Dispute Resolution

Operational escalation → senior escalation → (optional) mediation → courts. The Parties will continue performance where reasonably possible during dispute.

23. General

23.1 Assignment

Neither Party may assign the Contract without the other's written consent (not to be unreasonably withheld), except to a successor in connection with corporate reorganisation or sale of substantially all assets.

23.2 Severance

If any provision is invalid, remaining provisions continue.

23.3 Waiver

No waiver unless in writing.

23.4 Governing law

England & Wales.

SCHEDULE 1 — SERVICE SPECIFICATION (ASSET)

1. Overview

The Services provide a secure hosted platform and associated support to enable Virtual Schools / Local Authorities to manage and monitor:

- **ePEP** (Personal Education Plans for Children Looked After),
- **attendance monitoring**,
- **analytics and reporting**,
- progress tracking (including KS5 where applicable),
- exports in common formats to support internal reporting and statutory returns.

2. Modules / Components

1. **Platform Access (ASSET Core)**
 - role-based access, user management, audit trail (where enabled)
 - reporting dashboard and configurable reports
2. **ePEP for CLA / LAC**
 - workflows, templates, review cycles
 - evidence attachment/notes (as configured)
 - reporting outputs and monitoring views
3. **Attendance Monitoring**
 - collection mechanisms as agreed (manual uploads, secure data feeds, structured templates)
 - exception flags and monitoring dashboards
 - reporting outputs by cohort, school, period
4. **Analytics & Reporting**
 - unlimited report generation (subject to reasonable use)
 - exports: CSV/XLSX/PDF (where enabled)
 - scheduled reporting where configured
5. **Support & Guidance**
 - service desk support
 - training resources/video tutorials (where provided)
 - periodic platform updates included (free upgrades aligned to education change, unless otherwise stated)

3. Implementation Services

As per the Order Form, may include:

- onboarding plan and data mapping
- configuration and user setup
- initial training for key users
- go-live support period

4. Customer responsibilities (critical)

- provide agreed data extracts in agreed formats and timelines
- nominate key contacts and approvers
- ensure user accounts are managed and removed when no longer needed
- ensure lawful basis for processing and disclosures to Service Provider

5. Non-functional requirements

- reasonable availability aligned to SLA
- secure access controls and encryption in transit
- backup and disaster recovery arrangements (Schedule 8)
- retention and exit mechanics (Schedule 5)

SCHEDULE 2 — CHARGES & PAYMENT

1. Charging model

Charges are as set out in the Order Form and may be based on:

- number of schools/settings,
- number of users,
- LA-wide licence,
- modules enabled (ePEP, attendance, analytics),
- implementation services (if applicable).

2. Invoicing

- annual in advance / quarterly in advance / arrears: **[as per Order Form]**
- invoices reference the Order Form number and service period.

3. Price review / uplift (optional)

For renewals/extensions only, any uplift (if applied) shall not exceed CPI (ONS) unless scope is expanded via Change Control.

SCHEDULE 3 — SERVICE LEVELS (SLA) & SUPPORT

1. Support hours

Support Hours: [e.g., 09:00–17:00 UK Business Days]

Channels: [email / portal / phone]

2. Severity definitions

- **Severity 1 (Critical):** platform unavailable for all users or critical function unusable with no workaround.
- **Severity 2 (High):** major function impaired for many users; workaround exists.
- **Severity 3 (Medium):** issue affecting limited users or non-critical function.
- **Severity 4 (Low):** general query, cosmetic defect, how-to support.

3. Target response times

- Sev 1: response **1 hour**
- Sev 2: response **4 hours**
- Sev 3: response **1 Business Day**
- Sev 4: response **2 Business Days**

4. Target resolution / workaround times (targets, not guarantees)

- Sev 1: workaround/restoration **8 hours**
- Sev 2: workaround **2 Business Days**
- Sev 3: fix in planned release or **10 Business Days**
- Sev 4: planned release / advice

5. Availability target

Availability target: [99.5% / 99.9%] per calendar month, excluding planned maintenance.

6. Planned maintenance

- normally out of hours where possible
- notice: **5 Business Days** (or shorter for emergency security patching)

7. Service credits (optional)

If you want credits, insert them here (many LAs like them; some suppliers avoid them).

Default: No service credits unless the Order Form selects them.

8. Escalation

- First line: Service Desk
- Second line: Service Delivery Lead
- Third line: Senior Management escalation within **2 Business Days** if unresolved.

SCHEDULE 4 — DATA PROCESSING ADDENDUM (DPA)

1. Roles

Authority = Controller; Service Provider = Processor.

2. Subject matter, duration, nature and purpose

- **Subject matter:** hosting and operation of ASSET platform; support; reporting; attendance and ePEP processing.
- **Duration:** Term + Exit Period + **6 month retention** (Schedule 5), unless the Authority instructs earlier deletion.
- **Nature/purpose:** provide secure access, data storage, reporting/analytics, customer support, and configured workflows.

3. Types of Personal Data (typical)

May include (depending on configuration):

- pupil identifiers, demographic data
- school/settings data
- attendance records
- ePEP content, notes, assessments, interventions
- user account details and audit logs

4. Categories of Data Subjects

Children/young people, parents/guardians (where included), Authority staff, school staff.

5. Processor obligations

The Service Provider shall:

1. process only on documented instructions;
2. ensure confidentiality of persons authorised to process data;
3. implement TOMs (Schedule 8);
4. assist with subject rights requests and Controller obligations (reasonable assistance);
5. notify breaches without undue delay;
6. delete/return data per Schedule 5;
7. make available information necessary to demonstrate compliance and allow reasonable audits;
8. not appoint Sub-processors without approval mechanism below.

6. Sub-processors

- Pre-approved Sub-processors (if any): **[list here]**
- Changes: the Service Provider will notify the Authority of intended changes and provide a reasonable period to object on reasonable grounds (security/compliance). If objection cannot be resolved, Parties will discuss alternative approaches via Change Control or the Authority may terminate the affected part.

7. International transfers

No transfer outside the UK unless:

- Authority gives written instruction/approval; and
- an appropriate lawful transfer mechanism is in place (e.g., UK IDTA/UK Addendum), and security measures are maintained.

8. Breach notification

Notification will include (as available): nature of incident, categories/approx. volume, likely consequences, mitigation steps, and contact point.

SCHEDULE 5 — EXIT, DATA RETURN & RETENTION (6 MONTHS)

1. Exit trigger

Exit applies on expiry or termination (any reason).

2. Exit Period access

Unless termination is for security emergency, the Service Provider will provide an Exit Period of **30 days** to support orderly export/transition (or other period agreed in writing).

3. Data return

- Export formats: **CSV/XLSX/PDF** (where applicable) and any agreed structured extracts.
- Method: secure transfer mechanism agreed with the Authority.
- Assistance: reasonable assistance included as set out in Order Form; additional consultancy billed at agreed day rates (Schedule 2) where requested.

4. Retention (your requirement)

Authority Data will be retained for **6 months** after termination/expiry to allow retrieval, unless:

- the Authority requests earlier deletion; or
- legal/regulatory duties require longer retention for limited records (in which case those records are retained securely and minimally).

5. Deletion

After retention ends, data will be securely deleted in accordance with the Service Provider's deletion process and backup rotation, and deletion confirmation will be provided on request.

SCHEDULE 6 — ACCEPTABLE USE & SAFEGUARDING

1. Acceptable use

Authorised Users must:

- keep credentials secure;
- use ASSET only for lawful Authority purposes;
- not attempt unauthorised access, penetration testing, scraping, or disruption;
- not upload malicious code;
- comply with Authority policies where accessing from Authority premises/devices.

2. Safeguarding practice

- Staff are trained on handling sensitive pupil information and escalation routes.

- Any safeguarding concern identified in the course of service delivery is escalated via the agreed Authority safeguarding contact (or emergency route where immediate risk is identified).
 - Where on-site work occurs, Staff comply with school/Authority safeguarding protocols.
-

SCHEDULE 7 — CHANGE CONTROL PROCEDURE

1. Change Request

Either Party may submit a Change Request including:

- description and rationale
- impact on scope, time, Charges
- security/data protection impact (where applicable)
- dependencies and acceptance criteria

2. Assessment and decision

The Service Provider will assess feasibility and impact and respond within **10 Business Days** (or sooner if urgent).

3. Change Note

No Change is effective until a Change Note is signed by both Parties.

SCHEDULE 8 — SECURITY MEASURES (TOMs SUMMARY)

The Service Provider maintains measures appropriate for the nature of the data and risk, including:

- role-based access controls and least privilege
- secure authentication and password controls
- encryption in transit (TLS) and secure session management
- backup and recovery processes
- vulnerability management and patching
- logging and monitoring for security events
- staff confidentiality obligations and security awareness

- incident management process including breach response

(Where the Authority requires specific assurance artifacts, these are supplied on request subject to security constraints.)

SCHEDULE 9 — FOIA/EIR SUPPORT PROTOCOL

1. General

The Authority is subject to FOIA/EIR and remains responsible for responding.

2. Service Provider support

The Service Provider shall:

- notify the Authority within **2 Business Days** of receiving any FOIA/EIR request relating to the Contract;
- provide reasonable assistance and relevant information within Authority timelines;
- not respond directly to the requester unless authorised by the Authority or required by law.

3. Confidentiality vs disclosure

Nothing in the Contract prevents lawful disclosure. The Authority determines exemptions and public interest tests.

Order Form (template stub)

If you want this included as “page 1” like competitors, use:

- Authority name/address
- Service Provider name/address
- Effective Date
- Term (1/2/3 years)
- Modules enabled (ePEP, attendance, analytics, reporting)
- Charges and invoicing frequency
- SLA option (availability target, service credits yes/no)
- Key contacts / Contract Managers
- Special terms (if any)

869 High Road, London,
N17 8EY

Tel: +44 207 183 8357

<https://www.assetforschools.com>

COPYRIGHT © 2003-2026 Stat Solutions Ltd. All rights reserved. All materials in this document, including but not limited to logos, content, trademarks, artwork and associated imagery in this document are trademarks and/or copyright material of Stat Solutions Ltd and may not be reproduced, distributed, transmitted, displayed, published, broadcasted or stored in any form or by any means, including, but not limited to, electronic, mechanical, photocopy, record or otherwise