PUBLIC TRUST & ASSURANCE · PT-FIN-TERMS-001

Paulioskos Finance Terms of Use

Sets the rules and control boundaries for authorised use of the internal Paulioskos Finance platform, including HMRC Making Tax Digital functionality and future submission controls.

Version	Effective	Last reviewed	Owner
1.0	13 September 2026	13 September 2026	Company Directors & Finance Technical Owner

CURRENT RELEASE BOUNDARY

At v0.7.5 the HMRC integration is deliberately read-only: secure OAuth authorisation and VAT-obligation retrieval are implemented, but VAT-return calculation, preparation and submission are not. Any future write capability requires a separate controlled release and appropriate HMRC access.

Documents are reviewed periodically and whenever there is a material change to Finance functionality, controls, suppliers, legal obligations or risk profile.

Paulioskos Finance is currently an internal business system. These terms are published publicly for transparency and assurance; they do not constitute an offer of the platform as an accountancy, bookkeeping, tax-agent or software service to customers or other organisations.

1. Platform status and purpose

Paulioskos Finance supports controlled internal workflows including:

- customer and supplier financial records;
- quotations and commercial evidence;
- invoices and payment status;
- transaction recording and reconciliation;
- receipts and supporting evidence;
- accounting and VAT information;
- audit and approval records;
- reporting and reminders; and
- authorised HMRC Making Tax Digital functions where enabled.

The platform is operated for Paulioskos business administration and statutory financial/tax obligations.

2. Authorised users

Access is limited to people authorised by Paulioskos.

Users must:

- use their own approved identity;
- comply with assigned roles and permissions;
- protect authentication factors and devices;
- not share accounts, sessions or credentials;
- use the platform only for legitimate Paulioskos business purposes; and
- report suspected unauthorised access or security issues promptly.

Access may be restricted, suspended or removed where necessary for security, governance, employment/role changes, incident response or legal compliance.

3. Authentication and access control

Paulioskos Finance uses controlled authentication and role-based access.

Where Microsoft Entra ID is used, Microsoft operates the identity sign-in service. Paulioskos Finance does not need to store the user's Microsoft password.

Administrative functions are restricted according to role. Possession of an application account does not automatically grant unrestricted access to financial records, configuration or HMRC controls.

Users must not attempt to bypass authentication, authorisation, audit, segregation-of-duty or technical security controls.

4. User responsibilities and data accuracy

Users are responsible for taking reasonable care when entering, approving or changing financial information.

Users must:

- use appropriate source evidence;
- avoid knowingly creating false or misleading records;
- correct material errors when identified;
- preserve relevant supporting evidence;
- supply a meaningful reason where a controlled correction requires one; and
- follow applicable internal approval and reconciliation processes.

A system-generated total, status, warning or report does not remove the user's responsibility to review the underlying record where review is required.

5. HMRC Making Tax Digital

Paulioskos Finance is being developed for HMRC Making Tax Digital for VAT for **Paulioskos's own VAT account**. Paulioskos is not using the platform as a tax agent for third-party clients.

HMRC authentication is performed through HMRC's OAuth service. Users must not enter or store HMRC passwords inside Paulioskos Finance.

HMRC-supplied obligation information is authoritative for:

- obligation period keys;
- HMRC obligation status;
- HMRC due dates; and
- HMRC receipt or processing information where applicable.

Finance may derive operational labels such as **UPCOMING**, **DUE SOON**, **URGENT** or **OVERDUE** from HMRC data. These labels are workflow aids and do not replace HMRC's underlying status.

Finance must not treat a locally calculated quarter date as proof that HMRC has created a filing obligation.

Current release boundary

At version 0.7.5, HMRC integration is deliberately **read-only**. It supports secure authorisation and VAT-obligation retrieval but does not contain a VAT-return submission function.

No user should infer that a return has been filed merely because:

- an obligation is displayed;
- a reminder is sent;
- a due date passes;
- a local VAT calculation exists; or
- Finance displays a workflow status.

Any future VAT-return preparation or submission capability must be separately developed, tested, controlled and released.

6. Future VAT submissions

If a future approved release enables VAT submission, the following principles apply:

- submission must require valid HMRC authorisation and appropriate scope;
- users must review the VAT figures and period before submission;
- Finance must maintain durable evidence of the submitted period and result;
- a successful submission must not be silently or automatically repeated;
- submission identity must be bound to the environment, VRN and HMRC period key;
- HMRC acknowledgements/receipts must be retained as evidence where supplied; and
- submission failures must be visible and must not be represented as success.

The directors and authorised Finance users remain responsible for the accuracy and completeness of the company's VAT return.

7. Fraud-prevention information

HMRC requires VAT (MTD) API software to submit specified fraud-prevention header data. Paulioskos will not enable production HMRC use until the implementation has been checked against HMRC's current fraud-prevention specification and Test Fraud Prevention Headers API.

Where applicable, Paulioskos Finance may collect or derive technical information required by HMRC, including browser, device, user, connection and network attributes.

Users must not deliberately falsify, suppress or manipulate information required for HMRC fraud-prevention controls.

8. Prohibited use

Users must not use Paulioskos Finance to:

- access records they are not authorised to view;
- alter or conceal audit evidence improperly;
- submit false, fabricated or deliberately misleading financial information;
- disable or evade security controls;
- extract credentials, tokens, cryptographic material or secrets;
- introduce malicious code or unauthorised software;
- perform security testing outside an approved test/change process;
- use production HMRC credentials in an unauthorised development environment; or
- use the platform for another organisation's VAT account unless the platform and governance model are formally changed and approved for that purpose.

9. Environment separation and change control

Development and production environments are intentionally different.

Source control manages application code, migrations, controlled configuration examples, documentation and release artefacts.

Source control must not be treated as the repository for:

- production **.env** values;
- HMRC client secrets;
- token-encryption keys;
- OAuth access or refresh tokens;
- private certificates/keys;
- production databases;
- uploaded evidence; or
- other environment-specific secrets.

Production deployments must use controlled, approved release versions. Deploying application code must not overwrite or destroy live production databases, uploads or evidence.

Database migrations should be controlled, reviewed and backed up before application where required.

10. Audit and evidence

Paulioskos Finance maintains audit and operational evidence appropriate to controlled financial workflows.

Audit records may include:

- actor;
- time;
- operation;
- controlled change reason;
- success/failure state;
- correlation or provider reference; and
- application release/version.

Audit does not legitimise an otherwise unauthorised action.

Secrets such as passwords, client secrets, OAuth tokens and encryption keys must not be intentionally written to ordinary audit records.

Users must not tamper with or delete audit evidence outside an approved retention, maintenance or incident-response process.

11. Notifications and reminders

Finance may generate operational reminders, including VAT-deadline warnings.

Reminders are supplementary controls only.

Failure to receive a reminder does not remove Paulioskos's responsibility to meet statutory, contractual or payment deadlines.

HMRC status and official correspondence should be checked where there is any doubt.

12. Availability and maintenance

Paulioskos aims to operate Finance as a dependable internal business system but does not guarantee uninterrupted availability.

The platform may be unavailable because of:

- planned maintenance;
- upgrades or migrations;
- dependency/service-provider outages;
- security incidents;
- network or infrastructure failures; or
- emergency recovery activity.

Operational procedures should allow important statutory or financial work to be escalated where Finance is temporarily unavailable.

13. Backup and disaster recovery

When Finance is operated in production, its live data must be protected through controlled backup and recovery arrangements appropriate to its importance.

Recovery planning is intended to protect more than source code alone and includes, where applicable:

- PostgreSQL/application data;
- uploaded evidence;
- environment-specific configuration;
- certificates and cryptographic material;
- HMRC token-encryption material; and
- other state required to restore the service reliably.

Development recovery is separately protected using source control plus backup of non-source-controlled configuration/state.

Routine development backup procedures should not unnecessarily stop the WSL or Docker development platform.

Backup existence does not replace the need for periodic recovery validation.

14. Security

Users must follow Paulioskos security requirements and report suspected incidents promptly.

Paulioskos may:

- terminate sessions;
- revoke application access;
- rotate credentials or cryptographic material;
- disconnect HMRC authorisation;
- restrict network access; and
- preserve relevant logs/evidence

where reasonably required to contain or investigate a security incident.

15. Privacy and data protection

Personal information processed through Finance is handled according to the **Paulioskos Finance Privacy Notice** and related controlled Trust Centre material.

Users must access and use personal information only where necessary for their authorised role.

Information must not be exported, copied or shared merely because the platform technically permits access.

16. External services

Paulioskos Finance depends on services operated by third parties, which may include HMRC and Microsoft.

Those services are subject to their own availability, security controls, service terms and technical changes.

Paulioskos does not control HMRC’s tax systems, Microsoft’s identity platform or other external infrastructure.

A third-party outage or rejected API request must not be represented by Finance as a successful transaction.

17. Intellectual property and internal ownership

Paulioskos Finance, its source code, design, internal documentation and associated original material are owned by Paulioskos or used under applicable third-party licences.

Internal users receive only the access required to perform their authorised role. No right to redistribute, sublicense or commercially supply the platform is created by internal access.

Open-source and third-party components remain subject to their respective licences.

18. No replacement for professional or statutory responsibility

Paulioskos Finance is a business system. It does not replace:

- the directors' statutory responsibilities;
- HMRC guidance or formal HMRC records;
- professional accounting, tax or legal advice where such advice is required; or
- human review of material financial decisions.

Users must escalate uncertainty rather than relying blindly on a system-generated value or status.

19. Incident and error reporting

Users should promptly report:

- suspected data breaches;
- unexpected access;
- HMRC authorisation failures;
- incorrect VAT periods/status;
- duplicate or missing financial records;
- unexplained calculation differences;
- missing evidence;
- suspected security vulnerabilities; or
- incorrect system behaviour affecting statutory records.

Security vulnerabilities affecting a public Paulioskos service should follow the current Responsible Vulnerability Disclosure Policy where applicable.

20. Changes to Finance and these terms

Finance is developed under controlled versioning and release management.

These terms will be reviewed when there is a material change to:

- platform scope;
- HMRC permissions;
- VAT submission capability;
- user population;
- hosting;
- material suppliers;
- security model; or
- applicable legal/regulatory requirements.

Material changes will be published as a new controlled version.

21. Governing law

These terms and use of Paulioskos Finance are governed by the law of England and Wales.

Contact

Route	Details
Trust Centre	Open Trust Centre
Privacy enquiries	privacy@paulioskos.com
Security reports	security@paulioskos.com
Postal correspondence	Unit A, 82 James Carter Road, Mildenhall, IP28 7DE

Reference framework

These sources describe the legal, regulatory and good-practice framework used when preparing this document. They do not represent certification, accreditation, HMRC approval, regulatory endorsement or legal/tax advice.

Source	Link
HMRC Developer Hub - Terms of Use	Open source
HMRC - VAT (MTD) API 1.0	Open source
HMRC - Test Fraud Prevention Headers API 1.0	Open source
GOV.UK - Keeping VAT records	Open source
Paulioskos Trust Centre	Open source