



HOËRSKOOLOOS-MOOT

TENDER FOR IT SERVICES 2026

TENDER FOR IT SERVICES AT HOËRSKOOL OOS-MOOT

1. NOTICE TO SERVICE PROVIDERS

Service providers are hereby invited to tender for IT services at Hoërskool Oos-Moot. We require a smooth transition to a new tender arrangement **with effect from 1 December 2026**.

2. TENDER

2.1 Contract period

1 December 2026 to 1 December 2029

2.2 Tender closing date

6 November 2026

2.3 Site inspection

A site inspection may be arranged by email.

Contact person: Ms C Andrews (geboue@oos-moot.co.za).

2.4 Submission of tender

- Hoërskool Oos-Moot, 1120 Haarhoff Street, Villieria, Pretoria.
- A tender box will be available in the school's reception area.
- Tenders may be received on weekdays between **07:00 and 12:00** (excluding school holidays).

2.5 Documents to be included with the tender:

- Company letterhead
- Company profile
- Proof of banking details
- Proof of address
- Detailed terms and conditions
- References from previous clients
- Pricing structure and quotation
- Any additional supporting documents required

2.6 Evaluation and award

The tender will be evaluated by a panel of the governing body of Hoërskool Oos-Moot.

2.7 Tender submissions (envelopes) will only be opened after the closing date.

2.8 Tenders will be regarded as complete, and awards will be made solely on the basis of the information submitted.

2.9 Evaluation criteria

Tenders will be assessed on the following basis:

Criteria	Points allocation
1. Compliance with tender submission requirements.	5
2. Experience in providing similar services to schools and organisations.	25
3. Proven ability to deliver the required service.	25
4. Pricing structure and affordability	10
5. Reliability	30
6. References from previous or current clients.	5
TOTAL	100

2.10 Late submissions will not be considered.

- .
- 2.11 The governing body of Hoërskool Oos-Moot reserves the right to accept or reject any tender without providing reasons.
- 2.12 No applications by email will be accepted.

3. REQUIREMENTS

Attached as:

- Section 1 : CAT / IT
- Section 2 : Administrative, staff and network
- Section 3 : Optional value-added service (Laptop rental or financing model for teaching staff)

TENDER SUBMISSION DOCUMENT / FORM

HOËRSKOOL OOS-MOOT Tender for IT services Tender reference: HOSM-IT/2027

PART A: COMPANY INFORMATION

Please complete the details below:

1. Company name: _____
2. Trading name (if applicable): _____
3. Business registration number: _____
4. VAT registration number: _____
5. Contact person: _____
 - Title/Role: _____
 - Telephone: _____
 - Email address: _____
6. Physical address: _____

7. Postal address: _____

PART B: COMPLIANCE CHECKLIST

Please ensure that all the following documents are attached to your submission:

Document	Attached Yes/No	Comments
Company letterhead		
Company profile		
Proof of banking details		
Proof of address		
Detailed terms and conditions		
Detailed terms and conditions		
Pricing structure and quotation		
Additional supporting documentation		

PART C: DETAILS OF TENDER PROPOSAL

Provide detailed responses to the following:

1. Compliance with the requirements
Confirm compliance with the specifications set out in the invitation to tender. Attach supporting documents or proposals.
2. References
List at least three (3) references from previous or current clients. Include contact details and project descriptions.
3. Pricing structure
Provide a detailed quotation.

PART D: DECLARATION BY THE TENDERER

I, the undersigned, hereby confirm that the information provided in this tender submission is true and correct to the best of my knowledge. I further confirm that our company agrees to comply with the terms and conditions set out in the invitation to tender document.

Name : _____

Position: _____

Signature: _____

Date _____

Submission instructions

Submit the completed tender document, together with all required attachments, in a sealed envelope:

- a) Clearly mark it with the tender reference number HOSM-IT/2027
- b) Place of submission : Hoërskool Oos-Moot, Haarhoff Street, Villieria, Pretoria, 0186, in the tender box.
- c) Submission times : Between 07:00 and 12:00 (excluding weekends and school holidays).
- d) Closing date : 6 November 2026 at 12:00
- e) Late submissions will not be accepted.
- f) The governing body of Hoërskool Oos-Moot reserves the right to accept or reject the tender without providing any reason.

Enquiries may be directed to: Ms C Andrews (geboue@oos-moot.co.za)

SECTION 1:
SECTION 2
CAT AND IT NEEDS ASSESSMENT

1. PURPOSE

The purpose of this needs analysis is to ensure a comprehensive CAT and IT technical support service for the school. The service must focus on the effective management of CAT computer centres, examination support, technical maintenance, learner and examination profiles, and ongoing support for educators to ensure successful implementation of the CAT curriculum.

2. NEEDS ASSESSMENT

2.1 Learner profiles

- Creation and maintenance of individual learner profiles.
- Capture and management of learner data.
- Bulk creation or import of learner accounts where necessary.
- Password resets, account unlocking and restoration of damaged or corrupted user profiles.
- Assignment of users to the correct technical groups, access rights and folder permissions.
- Creation and maintenance of learner home folders, class folders and authorised shared folders.
- Management of appropriate storage quotas and access rights.
- Technical measures to prevent learners from opening other learners' private folders or obtaining administrator rights.

2.2 Examination profiles

- Development and maintenance of examination profiles in accordance with DBE requirements.
- Full-time technical support throughout the entire examination period.
- Support during the setup, testing and final preparation of examination venues.

Technical validation of learner logins, print client connectivity, examination folders, file permissions, printers, available server storage and backup status before practical assessments and examinations.

2.3 Examination support

- Creation, checking and validation of examination profiles in accordance with DBE specifications.
- Quality assurance of examination systems and digital files.
- Preparation and technical support during practical examinations.
- Immediate troubleshooting and problem resolution during examinations.
- Ensure that all computers, software and peripherals function optimally.
- Configure the internet network so that internet access is unavailable during examinations.
- Apply approved technical restrictions on cloud storage, USB devices, printers and folder access when required for an assessment or examination.
- Recover learner work where a technical session, thin client or server error causes a disconnection and a valid recovery source is available.
- Priority response when a technical fault prevents a practical assessment or examination from continuing.

Examination logins

The school requires unique learner logins, secure passwords, enough working computers, a stable network, access control and technical support. All user accounts and devices, as well as Office logins, must be tested before the examination. Software configurations must comply with DBE requirements.

The system must prevent unauthorised access and ensure that learners have access only to the required examination material.

- It must be possible to restrict devices so that learners cannot access unauthorised programs, websites or files.
- An IT person must be available to resolve login or computer problems quickly.

Examination files and important data must be backed up regularly.

Before the examination:

1. Create/verify all learner accounts with secure passwords.
2. Check that each learner's username works.
3. Test all computers.
4. Test network and internet connectivity.
5. Ensure that the correct examination software is available and that its configuration meets the requirements.
6. Activate the necessary security/examination restrictions.

During the examination:

1. The learner logs in using their own details.
2. The learner has access only to the examination and permitted resources.
3. Login problems are handled by the IT person.

After the examination:

1. Ensure that all answers have been saved correctly.
2. Confirm that files have been submitted.
3. Back up the examination files.

2.4 Full-time IT support

- Daily technical support for educators.
- Installation, configuration and verification of software for daily use.
- Support for Microsoft Office and Microsoft 365.
- Technical support during school hours.
- General user support for staff and learners.
 - Installation, updating and troubleshooting of programs used by teachers
 - Regular maintenance and updating of staff computers and laptops.
 - Antivirus, security updates, access control and protection against cybersecurity threats.
 - Support with secure storage and backup of important school and teacher data.
 - Preparation and technical support during CAT/IT practical examinations.
 - Practical training for teachers on new software, devices and digital tools.
 - A simple system through which teachers can report and follow up on technical problems.
 - Regular equipment checks to prevent problems before they disrupt teaching.

2.5 Technical Support and Maintenance

- Management and maintenance of CAT computer laboratories.
- Updating and licence management of Microsoft Office and Microsoft 365.
- Network, internet and domain support.
- Troubleshooting of computers and peripherals.
- Support for printers, projectors and other audiovisual equipment.
- Management of user accounts and access rights.
- Data backup and recovery processes.
- Preventive maintenance of all equipment.
- Preparation of laboratories for assessments and examinations.

- Software configuration to prevent learners from playing internet games when internet access is blocked by classroom control software.
- The IT laboratory must receive technical support for Embarcadero Delphi, Microsoft Access, Microsoft Word, Excel and PowerPoint, Scratch, Google Chrome, Google Classroom, Google Drive, Gmail/Department of Education Google accounts and PDF software.
- The four CAT laboratories must receive technical support for Microsoft Word, Excel, PowerPoint and the full version of Microsoft Access, as well as Google Chrome, Google Classroom, Google Drive, Gmail, Google Docs, Sheets, Slides, Forms and PDF software.
- All approved applications must be correctly installed, activated and licensed; open for authorised users; create, open and save files; and print to the correct network printer where necessary.
- Software must remain compatible with the server, operating system, thin client and security environment and must not be incorrectly blocked by antivirus, firewall, profile or folder permissions.
- Delphi must be able to create, open, save, compile and run valid projects, with the required standard components and libraries available. The service provider is not responsible for debugging learner code.
- The full version of Microsoft Access must be available and functional; Access Runtime alone is not sufficient for CAT and IT purposes.
- Google services must be technically accessible from the laboratory environment, including uploading and downloading files, subject to Department of Education account permissions and the availability of external Google services.

2.5.1 *IT Wise thin client and server support*

- Configuration and connection of existing IT Wise thin clients to the correct server environment.
- Resolution of login, connection, freezing and disconnected session errors on thin clients.
- Maintenance of device names, network settings and approved firmware or software configurations.
- Technical troubleshooting of screen, keyboard, mouse, audio and approved USB functionality.
- Monitoring of server availability, processor usage, memory usage, storage capacity and active user sessions.
- Management of Remote Desktop or similar services, user profiles, temporary files, folder permissions and storage quotas.
- Restarting failed technical services and resolving server-related access problems.
- Ensure that all four laboratories can operate simultaneously without avoidable server-related performance problems.
- Liaison with IT Wise or an appropriate provider where specialised supplier support is required.
- No major change to the server, thin client, security or network configuration that could affect teaching, assessment or examinations may be made without school approval.

2.5.2 *Network, internet and printer support*

- Technical support for network switches, cabling, network points, server network connections, routers, firewall rules, DNS and DHCP services serving the laboratories.
- Troubleshooting internet connectivity and liaising with the internet service provider where necessary.
- Support for network printer connectivity, print queues and printing from approved applications.
- Diagnosis of whether a technical fault originates in the school network, server, thin client, internet service provider, Google service, Department system or local software configuration.

- Where a Google account problem requires administrative rights that the school does not hold, the service provider must help identify the technical cause and escalate the matter to the appropriate Department of Education support channel. Department-controlled domain settings or accounts may not be changed without authorisation.

2.5.3 Backup, recovery and preventive maintenance

- Monitoring successful backup processes and investigating failed backups.
- Periodic testing to ensure that backed-up files can actually be restored.
- Restoration of learner, teacher, shared or examination files where a valid backup exists.
- Immediate reporting of backup failures or capacity risks to the school.
- Maintaining documentation on backup locations and applicable retention periods.

Preventive checks of server health, capacity and error logs; thin client connectivity; network and printer connectivity; software activation; antivirus/endpoint security; system updates; user profiles; temporary files; storage capacity and backup status.

Maintenance and technical support

Technology must be maintained regularly to limit problems and downtime. A maintenance plan may include:

Daily:

Check that important systems are functioning.
Report technical problems.

Weekly:

Check for network and internet problems.
Check available storage space.

Monthly:

Install updates.
Check security software.
Check computer equipment.

Annually:

Evaluate the age and condition of equipment.
Determine which equipment must be replaced.
Prepare a budget for new technology.

2.6 Teacher development

- Training in Microsoft Office and Microsoft 365.
- Support with new technology and digital teaching.
- Individual technical support and mentoring for educators.

2.7 Prioritisation of technical support

- Critical: Main server unavailable; all laboratories offline; a practical examination cannot continue; or a widespread login or network fault. Immediate technical investigation and escalation are required until service is restored or a workable technical solution is implemented.
- High: An entire laboratory is offline; Delphi is unavailable for the IT class; Microsoft Office is unavailable for a CAT class; several users cannot log in; or an assessment printer is unavailable. Same-day technical attention is required.
- Normal: A single thin client fault, one user profile requiring restoration, a single printer connection fault or an isolated non-critical software installation problem. This must be resolved through the agreed normal support process.

2.8 Technical reporting and documentation

- Maintaining records of reported, resolved and outstanding faults, as well as recurring laboratory, server, network and thin client problems.
- Recording server, backup and software availability issues and technical maintenance performed.
- Maintaining an up-to-date list of relevant laboratory devices, printers and servers, as well as the network and IP information needed to support the laboratories.
- Maintaining applicable software licence information and administrator, configuration and support documentation.
- All school accounts, administrator credentials, configurations, data and technical documentation remain under the ownership and control of the school. The service provider may not prevent the school from accessing its own systems or data.

3. Deliverables

The service should provide the following deliverables:

- Complete and updated learner profiles.
- Accurate examination profiles in accordance with DBE requirements.
- Full-time technical support during examination periods.
- Effective management of CAT computer laboratories.
- Reliable network and software support.
- Reduced technical downtime.
- Improved functioning of computer facilities.
- Increased readiness for NSC practical examinations.
- Efficient support for educators and learners.
- Professional maintenance of all CAT and IT infrastructure.

- Reliable technical availability of the existing IT Wise thin client, server, network, printer and software environment for all four laboratories.
- Clear technical documentation and retention of school control over accounts, configurations, data and administrator access.
- A full-time IT support service.
- An IT maintenance and backup plan.
- A cybersecurity and data protection plan.
- A training plan for teachers.
- A budget for new and replacement IT equipment.
- A priority list of needs to be addressed urgently, in the medium term or in the long term, together with the associated budget
- A system through which teachers can report problems and monitor repair progress.

SECTION 2

ADMINISTRATIVE, STAFF AND NETWORK IT TECHNICAL NEEDS ANALYSIS

SCOPE OF THIS SECTION: This document covers administrative and staff IT, telephones, network, Wi-Fi and related infrastructure. The CAT and IT classrooms are addressed in a separate needs analysis. Where shared infrastructure (e.g. network, internet or cabling) affects both sections, the two sections must be coordinated without duplicating responsibilities.

1. PURPOSE

The purpose of this needs analysis is to set out the school's requirements for a comprehensive, reliable and professionally managed IT support service for administrative staff, heads of department and educators. The service must include daily user support, telephony, network and internet infrastructure, Wi-Fi, system support, asset and licence management, documentation, preventive maintenance, budget planning and technical risk management.

The school requires a service provider that manages the environment proactively as well as responding to faults, identifies problems early, protects the school's technical assets and can develop a sustainable three-year maintenance and replacement plan.

2. NEEDS ASSESSMENT

2.1 Full-time support on the school premises

- A dedicated IT technician must be available full-time on the school premises from 08:00 to 16:00 on the agreed service days and provide support for both Section 1 (CAT/IT classrooms) and Section 2 (administration/staff/network).
- The person on site must be the first technical point of response for both Section 1 and Section 2 and have sufficient knowledge to diagnose and resolve, or correctly escalate, general desktop, network, Wi-Fi, telephony, printer connectivity, classroom and system problems.
- The service provider must ensure continuity when the designated technician is on leave, ill or otherwise absent. A suitable replacement must be available without interruption to the school's support.
- The designated technician may not regularly be withdrawn from the premises to work for other clients without prior school approval.
- The full-time on-site technician is not solely responsible for the entire service scope. Where a problem exceeds the technician's expertise or capacity, specialised second- or third-level support is required, or several urgent problems occur simultaneously, the service provider must make additional technical staff available virtually or physically. The service provider as a whole remains responsible for escalation, follow-up, resolution and feedback until the matter is concluded.
- The service provider must have sufficient internal capacity and backup staff so that service delivery does not depend on one individual technician; virtual support, remote troubleshooting and additional on-site support must be used where they offer the quickest or most appropriate solution.
- Professional conduct, confidentiality, orderly documentation and respect for school processes are core requirements.

2.1.1 Continuity and support outside normal school hours

- The tenderer must indicate in their proposal what support is available for critical IT incidents outside normal on-site hours, particularly during practical examinations, important school functions, registration processes or other critical operating periods identified in advance.
- The tenderer must set out the procedure and contact/escalation route for such support, together with any applicable conditions or additional costs.

- Where the designated on-site technician is unexpectedly absent, the service provider must ensure continuity and indicate in the tender response how replacement or alternative support will be provided.

2.2 General desktop and user support

- Daily technical support for administrative staff, heads of department and educators using school-approved computers and laptops.
- Troubleshooting of Windows, Microsoft Office/Microsoft 365, browser, PDF, email, login, profile, peripheral and general workstation problems.
- Installation, configuration and updating of approved software and drivers.
- Setup of new or replacement computers, including user profiles, network access, approved programs, printers and security settings.
- Migration of user data to new devices where necessary and authorised by the school.
- Basic troubleshooting of keyboards, mice, monitors, docking stations, webcams, audio and other approved peripherals.
- Support with password resets, account access and appropriate user rights in accordance with the school's authorisation process.
- Regular updating and preventive maintenance of staff devices to limit downtime.
- No administrator rights or permanent technical workarounds may be granted to individual users without written school approval.

2.2.1 Staff members' personal electronic devices

For the purposes of this tender, this also includes staff members' personal electronic devices, e.g. computers and laptops belonging to educators, heads of department and administrative staff, where these devices are approved by the school and used for official school and teaching purposes.

The IT service provider must be able to provide reasonable first-level technical support for these devices, including:

- connection to the school's approved Wi-Fi and network services;
- connection to data projectors, visualisers, printers and other approved classroom equipment;
- installation and configuration of school-approved software;
- support for Microsoft 365, Google Workspace and other approved digital platforms;
- basic troubleshooting of Windows, login, profile, email, software and connectivity problems;
- installation of appropriate drivers and security updates where necessary; and
- basic fault diagnosis and recommendations where hardware repair or replacement is necessary.

The service provider is not automatically responsible for the cost of parts, licences, hardware repairs or replacement of staff members' personal electronic devices. Any such costs remain the responsibility of the staff member concerned, unless otherwise agreed.

The IT service provider must exercise reasonable care when working on staff members' personal electronic devices and may not carry out any reformatting, data deletion or other substantial change without the consent of the staff member concerned and, where applicable, the school's authorised IT coordinator.

2.2.2 Data projector support

The school prefers the new IT service provider to be able to take over technical support and general maintenance of data projectors. This capability is desirable and will be regarded as an advantage, but a tenderer will not be excluded from the tender process or disqualified if they cannot provide data projector support.

- Tenderers must clearly confirm in their proposals whether data projector support falls within their capabilities and service scope.
- Where offered, support must include general troubleshooting, connection to staff devices, basic configuration, lamp/image/signal problems, cabling work (installation of projectors, HDMI cables, connection points, etc./fault-finding/replacement of filters, lamps, cables, connection points, projectors, etc.) and liaison for repair or replacement, within the limits of the service provider's technical capabilities.
- **If the tenderer cannot provide this service, the school reserves the right to have data projectors supported by a separate person or service provider, without necessarily affecting the tenderer's suitability for the core IT service.**

2.3 Fixed telephones and 3CX telephony

The school currently has 35 fixed telephone devices/extensions used mainly by administrative staff and heads of department, together with the 3CX telephone program/application. The new service provider must be able to take over the technical management and support of this environment.

- Management and support of the existing 3CX environment, extensions, devices and users.
- Configuration of new users, extensions and approved 3CX application access.
- Support with call routing, ring groups, transfers, voicemail, general call flow and appropriate reception functions.
- Troubleshooting devices that fail to register, have no audio, drop calls or experience network/internet-related call problems.
- Updating firmware and software where applicable and following approval.
- Liaison with the telecommunications, SIP, internet or other relevant third-party provider when the fault lies outside the school network or 3CX configuration.
- Maintaining an up-to-date list of devices, extensions, users, IP information and core configuration.
- All 3CX administrator access, licence information, recovery details and technical documentation must remain under the school's control.
- Any licence, trunk, call or third-party costs that are not included in the service fee must be clearly identified in advance and listed separately.

2.4 Staff and departmental printers

Administrative staff and heads of department use individual or departmental printers. These printers are serviced by Daisy under an existing contract. The new IT service provider is therefore not responsible for mechanical servicing, toner, consumables or repairs to these printers, but must support the network and user side.

- Configuration of network connectivity, fixed IP settings where applicable, print ports, drivers and user connectivity.
- Troubleshooting print queues, network printing, permissions and users who cannot print to an approved printer.
- Diagnosis of whether a fault originates in the user device, school network or the Daisy-serviced printer itself.
- Where the fault lies with the printer or the existing Daisy contract, the service provider must escalate the matter correctly and cooperate with Daisy to resolve it.
- No service provider may replace, amend or duplicate existing printer SLAs without express school approval.

2.5 Network, fibre, switches and internet

- Full technical management and support of the school's general network serving administration, staff and shared school services.

- Support and monitoring of fibre/internet connectivity, routers, firewalls, core and edge switches, network points, patch panels, cabling and other relevant network components.
- Management of DNS, DHCP, IP, VLAN and other appropriate network services within the school's authorised environment.
- Troubleshooting internet and network outages and liaising with the internet/fibre service provider where necessary.
- Maintaining an up-to-date network diagram, IP plan, list of switches, access points and network devices, and important port/connection information.
- Clear labelling and documentation of critical network points, patching and equipment where practicable.
- Proactive monitoring of capacity, error logs, availability and recurring network problems.
- No major change to VLANs, firewall rules, core switches, internet routing or other critical network settings may be made without prior school approval.
- All configuration backups, administrator details and network documentation must be available to the school and updated regularly.

2.6 School Wi-Fi and control of unauthorised learner access

The school's Wi-Fi is intended for authorised staff and approved school use. Learners should not have general access to staff/administrative Wi-Fi. The school currently has a problem with learners obtaining or using Wi-Fi credentials. The service provider must propose and implement a practical, sustainable and secure solution, subject to school approval.

- Management, monitoring and maintenance of wireless access points, controllers/cloud management, SSIDs, coverage and network connectivity.
- Segregation of administrative, staff, guest and other approved wireless networks where necessary.
- An access model that limits the sharing and reuse of a single staff password as far as reasonably possible, for example individual or device-based authentication, certificate/identity-based access or another suitable solution.
- Restriction or isolation of unauthorised devices and clear procedures for adding/removing authorised devices.
- Temporary, controlled guest access where required by the school, without access to internal administrative resources.
- Monitoring unusual usage, recurring connection problems, rogue/unauthorised access attempts and capacity problems, with appropriate reporting to the school.
- The solution must be user-friendly for staff and may not depend on a single shared password if a safer, practical alternative is available.

2.7 Cybersecurity, access and change control

- Basic endpoint security, antivirus/anti-malware, security updates and appropriate system patching for school-approved devices.
- Strong control of administrator accounts, with the minimum necessary privileges and multifactor authentication where supported by the system.
- Support with identifying and handling malware, phishing, compromised accounts and other technical security incidents.
- Timely deactivation or amendment of access when staff leave the school, change roles or no longer require access, on the instructions of an authorised school representative.
- No new remote access tool, agent, administrator account or permanent backdoor may be installed on school systems without approval.

- All significant changes to core systems, network, firewall, Google Admin, 3CX or server/sharing settings must be recorded with the date, reason, responsible person and relevant configuration details.
- The service provider must make technical recommendations to reduce risk, but changes with a significant impact must be approved by the school.

2.7.1 Cybersecurity incidents and data protection

- The service provider must propose and apply a clear technical response process for malware, ransomware, phishing, compromised accounts, suspected data breaches and other serious security incidents.
- An affected device or account must, where appropriate, be isolated or secured as soon as possible to limit further exposure or spread.
- Serious incidents must be reported to the school's authorised representative without unreasonable delay, with a record of the incident, steps taken, possible impact and recommended follow-up actions.
- The service provider must provide reasonable technical support to preserve relevant logs, technical evidence and recovery information where required for investigation, data protection or any applicable POPIA process.
- The service provider and its staff must treat all personal, learner, staff, financial and administrative data they access as confidential and access it only for authorised technical purposes.

2.7.2 Remote access

- Only school-approved *remote access* tools, agents and accounts may be used.
- *Remote access* must, where technically possible, be controlled through named user accounts, appropriate strong authentication and a traceable access log.
- Permanent or uncontrolled *remote access* to school systems may not be created without express school approval.
- *Remote access*, agents and accounts that are no longer required or authorised must be securely removed or deactivated.

2.8 Administrative systems and applications

The service provider must be able to provide technical support for the school's core administrative applications. The service provider does not have to be the functional owner or software developer of every system, but must perform first-level technical troubleshooting, rule out local/network problems and escalate to the relevant software provider where necessary.

- **Action Timetable:** Support for installation, access, network sharing and the current shared setup made available from a laptop/"server" computer.
The existing setup must be evaluated for reliability, backup and single-point-of-failure risk, with an improvement proposal where necessary.
- **d6:** Technical support with access, local installation/web access, user problems and escalation to d6 where the fault lies with the platform.
- **Google Admin / Google Workspace:** Management and support of authorised users, groups, aliases, passwords, access rights, MFA and appropriate administrative settings within the school's control. Department-controlled accounts or domain settings may not be changed without authorisation.
- **WordPress / school website:** Technical maintenance of the WordPress environment, including user/administrator access, core/plugin/theme updates, technical troubleshooting, backups, security, SSL/domain/hosting liaison and recovery following technical problems.

Daily content creation or website redesign does not automatically form part of the core scope unless separately agreed.

- **Microsoft 365 / Office and general office programs:** Technical support with installation, licence/login problems, email/profile problems, file access and general office productivity software.

2.9 Account, licence and administrator management

- Maintaining a register of relevant software licences, renewal dates, providers, licence keys/portals and the responsible school contact.
- All core administrator accounts must, where possible, use school-controlled email addresses and must not belong exclusively to an individual technician or service provider.
- The school must at all times have access to core administrator credentials, recovery methods and the documentation needed to take over its own systems.
- Passwords and sensitive access details must be stored securely and made available only to authorised persons.
- The service provider may not create a technical or contractual dependency that prevents the school from appointing another service provider or accessing its own systems.

2.10 Data backup, recovery and continuity

- Identification of critical local data, shared folders, configurations and other data for which the school is responsible.
- Development and maintenance of an appropriate backup and recovery plan for data and configurations not already protected by an external platform/provider.
- Monitoring backup success and immediately reporting failed backups or capacity risks.
- Periodic testing to ensure that critical backups can actually be restored.
- Documentation of backup locations, responsibilities, retention periods and recovery procedures.
- Preparation of a basic recovery/continuity plan for core network, internet, telephony and administrative functions.

2.10.1 Backup standards and recovery testing

- As part of their proposal, the tenderer must recommend an appropriate backup model for the school's relevant local data and critical configurations, with proposed backup frequency, retention periods, backup locations and responsibilities.
- Where applicable, the model must provide for critical backups to be kept somewhere other than solely on the same physical device or at the same location as the original data.
- Recovery tests must be performed and documented regularly on an agreed basis to confirm that critical backups are usable.
- Failed backups, capacity risks or any condition that could prevent reliable recovery must be reported to the school without unreasonable delay.

2.10.2 Disaster Recovery and Business Continuity Plan

- The tenderer must propose a practical recovery and continuity approach for the loss or unavailability of critical IT services, including the core network, internet connectivity, important network equipment, telephony, critical administrative systems and relevant local data.
- The proposal must indicate at least the main recovery priorities, dependencies, responsible parties, temporary workable alternatives and proposed recovery targets. Final recovery targets and responsibilities will, where applicable, be set out in the final SLA.

2.11 IT asset, purchasing, warranty and insurance support

- Maintaining and regularly verifying an up-to-date IT asset register for relevant administrative/staff equipment, including at least device type, make/model, serial number, asset/tag number, user or location and status.
- Maintaining purchasing information where available, including purchase date, supplier, invoice/reference, cost and related documentation.
- Maintaining warranty information, warranty expiry dates and proof of purchase, and using warranty channels before incurring unnecessary repair/replacement costs.
- Technical assistance with purchases: preparing minimum specifications, assessing technical suitability and comparing solutions in accordance with the school's approved procurement process.
- No purchase or order may be placed by the IT service provider on behalf of the school without appropriate school authorisation.
- Support in maintaining the school's insurance schedule for IT assets by keeping accurate asset details, serial numbers, proof of purchase and other technical information available.
- Assistance with technical documentation for insurance claims, damage reports, replacement specifications and confirmation of device identity when necessary.
- Records of written-off, replaced, stolen, damaged or relocated equipment must be reported to the school so that the asset register and insurance information can be updated.

2.12 Preventive maintenance and regular inspections

The service must include a structured preventive maintenance programme in addition to fault-driven support. The programme must cover at least the following:

- Daily: checking critical network/internet/telephony availability and urgent outstanding problems.
- Weekly: reviewing recurring tickets, network/Wi-Fi faults, critical capacity or connectivity problems and core backup/system alerts.
- Monthly: sampling/inspection of equipment, updates, security status, access points, switches, storage/capacity issues and documentation.
- Quarterly: a formal technical condition review of core infrastructure and identification of equipment requiring repair, upgrading or replacement.
- Annually: a full lifecycle and replacement assessment for budgeting and the three-year plan.

2.13 Cabling and Department of Education Memo 416 of 2025

All new network cabling, network points, patching, installation work and related infrastructure changes must comply with the applicable Department of Education specifications and guidelines, including Memo 416 of 2025. The school will provide Memo 416 of 2025 as an attachment to the tender. The service provider must study the memo and incorporate compliance into every installation, quotation or technical proposal.

- No deviation from the departmental specification may occur without prior school approval.
- New cabling must be neatly installed, tested, labelled and documented, with test results/certification where required by the applicable specification.
- The service provider must report existing cabling risks or non-compliant work identified during support to the school in writing.
- Attachment to the final tender: Department of Education Memo 416 of 2025, including the applicable cabling and network infrastructure specifications.

2.14 Communication channels, work allocation and ticket system

The school requires a clear communication structure to prevent uncoordinated instructions, duplicated work and loss of accountability. Staff may report technical problems, but individuals may not directly

reprioritise the service provider's or on-site technician's work or assign new work outside the approved process.

- Section 2 (administration/staff/network): all work is channelled and prioritised through the school's designated coordinator (currently Charmaine Andrews).
- Section 1 (CAT/IT classrooms): all work is channelled and prioritised separately through the designated CAT/IT coordinator/HOD (currently Natasja Pfeil).
- The two coordinators must have access to the ticket system and be able to manage their respective workflows separately, while coordinating shared infrastructure problems.
- No individual staff member, head of department, teacher or other user may bypass the on-site technician's work priorities by issuing instructions directly.
- Critical emergencies may be brought to the technician's attention immediately, but must be recorded as a ticket and communicated to the relevant school coordinator as soon as possible.
- All tickets must contain a date, user/location, description, priority, responsible technician, status and closure note.
- Tickets may not be closed as "resolved" without a meaningful note describing what was done or the outcome.
- Quotations, infrastructure changes, purchases and any work resulting in additional costs require prior approval by an authorised school representative.

2.14.1 Closure of support requests and confirmation of resolution

- Where practicable, the user concerned or designated school coordinator must have an opportunity to indicate if a problem has not actually been resolved.
- A *ticket* closed as resolved must be capable of being reopened if the same problem persists within a reasonable period or recurs immediately.
- Recurring problems must be identified in the monthly report so that the underlying cause can be investigated, rather than dealing only with each individual symptom separately.

2.15 Prioritisation and escalation of technical support

- Critical: School-wide internet/network outage; core telephony unavailable; a serious security incident; or a critical administrative function cannot continue. Immediate investigation, communication and escalation are required until service is restored or a workable temporary solution is implemented.
- High: An entire office/department or several users are affected; an important system is unavailable; or a network/Wi-Fi fault affects significant school operations. Same-day technical attention is required.
- Normal: A single user, device, printer connection, software installation or other isolated problem that does not stop core operations. This must be handled through the agreed normal SLA process.
- Planned: Upgrades, new installations, cabling work, replacements, migrations and other non-urgent changes are planned and approved in advance.

2.15.1 Proposed SLA response, escalation and resolution times

- As part of the tender response, the tenderer must indicate their proposed service levels for each priority category set out in clause 2.15.
- The proposed service levels must be realistic, measurable and achievable, and must distinguish at least between the following:
 - Response time: The maximum time from the correct reporting of a technical problem until the service provider acknowledges it and begins technical investigation or support.

- Escalation time: The maximum time after which a problem must be escalated to appropriate second- or third-level support or a relevant third-party provider if the first-level/on-site technician cannot resolve it through the normal support process.
- Target resolution time: The period within which the service provider reasonably aims to resolve the problem fully or, where a final solution is not immediately possible, implement a workable temporary solution.

The tenderer must complete the table below:

Priority	Proposed response time	Proposed escalation time	Proposed target resolution time
Critical	_____	_____	_____
High	_____	_____	_____
Normal	_____	_____	_____
Planned	_____	_____	_____

- The tenderer must clearly set out in the tender response any conditions, exclusions or dependencies that may affect the proposed times.
- Where the final resolution depends on a third-party provider, internet service provider, software provider, warranty repair, availability of parts or another factor outside the IT service provider's direct control, the service provider must remain responsible for correct escalation, follow-up and regular feedback to the school until the problem is resolved.
- The proposed service levels will be considered during tender evaluation, and the final response, escalation and resolution times will, following agreement between the school and the successful tenderer, be recorded in the final service level agreement (SLA).

2.16 Supplier and third-party management

- Where necessary, the IT service provider must liaise on behalf of the school's technical team with internet/fibre providers, Daisy, software providers, hosting/domain providers, 3CX/telecommunications providers and other relevant technical parties.
- The service provider remains responsible for managing and following up on a problem where its cause lies with a third party; the ticket may not simply be closed because another provider is involved.
- The school must be informed of expected costs, dependencies and any decision it needs to make before paid third-party work is authorised.

2.17 Technical documentation and reporting

- Maintaining records of reported, resolved and outstanding problems, including recurring fault patterns.
- Monthly reporting to the designated school coordinators covering at least: ticket volumes, critical/high-priority problems, outstanding items, recurring problems, network/Wi-Fi issues, important changes, risks and recommendations.
- Maintaining the network diagram, core IP/VLAN information, firewall/router/switch/AP inventory and relevant configuration documentation.
- Maintaining an IT asset register, licence register, warranty register, purchasing records and relevant supplier/SLA information.
- Documentation of important recovery procedures, backup status and critical administrator access.
- All documentation created in performing the service and relating to the school's own environment must be available to the school.

2.18 Annual budget requirements and three-year IT plan

- Each year during June, by a date determined by the school, the service provider must submit a structured statement of IT budget requirements for the next budget cycle.
- The budget proposal must indicate urgency, technical justification, estimated cost, risk if deferred and recommended timeframe.
- A rolling three-year plan must be developed and reviewed at least annually for maintenance, replacement, upgrades, licences, network/Wi-Fi, telephony, security and other relevant infrastructure.
- The three-year plan must classify equipment according to urgent, medium-term and long-term priorities and indicate lifecycle/replacement dates where possible.
- Unexpected major risks arising outside the annual budget cycle must be reported to the school immediately in writing and may not be held over until June.

2.19 Knowledge transfer and staff support

- Short, practical training for staff when new approved systems, security measures or working methods are introduced.
- Simple user guidelines for recurring problems where these can reduce ticket volumes.
- Knowledge may not remain with only one individual technician; the service provider must maintain internal documentation so that support can continue when staff change.

2.19.1 IT orientation for new staff

- On authorised instructions from the school, the service provider must support new staff through a simple, documented IT onboarding process.
- Where applicable, the process must include setting up or verifying user accounts, email/Google/Microsoft access, Wi-Fi, 3CX, network and printer connectivity, approved software, relevant shared resources and basic security requirements.
- Access must be assigned according to the staff member's role and the principle of least privilege.

2.20 Handover, contract termination and school control

- The school remains the owner/controller of its accounts, data, configurations, documentation, passwords and technical environment.
- On contract termination or a change of provider, a structured handover must take place without unreasonable delay or withholding of information.
- The handover must include relevant administrator credentials, configuration backups, network diagrams, asset/licence/warranty registers, outstanding *tickets*, third-party contacts and other critical technical documentation.
- Any provider-specific remote agents, accounts or access that are no longer authorised must be securely removed or deactivated after the handover.

2.20.1 Staff offboarding and termination of access

- When a staff member leaves the school, changes roles or no longer requires access, appropriate digital access must be deactivated, amended or revoked promptly on authorised instructions from the school.
- Where applicable, the process must cover school-controlled email/Google/Microsoft accounts, Wi-Fi, 3CX, shared folders, administrator or system access, remote access and other relevant school services.
- Where school data is present on a device or account, the school's authorised representative must determine how it is to be preserved, transferred or removed before access is finally terminated.
- The service provider must keep a simple record of the technical offboarding steps completed.

3. CLEAR EXCLUSIONS AND SEPARATE SERVICES

3.1 Large photocopiers / multifunction copiers

The school's large photocopiers/multifunction copiers are covered by a separate service level agreement (SLA) and are expressly excluded from this tender. They are not an alternative or optional part of this tender, and tenderers must not include any service, rental, replacement or maintenance pricing for these machines in the core proposal.

3.2 CAT and IT classrooms

The CAT and IT classrooms, learner profiles, examination profiles and specific classroom/examination support are addressed under Section 1 of the tender and the separate CAT and IT technical needs analysis. The Section 2 service provider must, however, cooperate where the general network, internet, fibre, firewall, cabling or other shared infrastructure affects both sections.

4. THREE-MONTH TRIAL PERIOD AND SERVICE PERFORMANCE

Initial service delivery will be subject to a three (3) month trial/performance evaluation period. During this period, the school will determine whether the service provider can maintain the required level of technical competence, availability, communication, documentation and professional service.

- Attendance and reliability of the full-time *on-site* technician (08:00–16:00).
- Compliance with the ticket and communication process.
- Quality and speed of troubleshooting and escalation.
- Ability to handle network, Wi-Fi, 3CX, desktop and administrative system problems professionally.
- Accurate documentation, record-keeping and feedback.
- Preventive management rather than exclusively reactive support.
- Professional conduct, confidentiality and cooperation with staff and third-party providers.

The final tender/service level agreement must specify the corrective steps, performance improvement process or termination rights that apply if the service provider fails to meet the agreed requirements during the trial period.

4.1 Ongoing SLA performance measurement

- After the three-month trial period, service performance must be monitored continuously against the final SLA.
- Where the ticket system allows, the monthly service report must indicate at least the following:
 - total number of tickets and number of tickets per priority level;
 - percentage of tickets handled within the agreed SLA response and resolution targets;
 - average response time and average resolution time;
 - critical and high-priority incidents, with the relevant cause and follow-up;
 - outstanding, reopened and recurring problems; and
 - any service level deviations, reasons for them and proposed corrective action.
- Repeated or significant non-compliance with the agreed SLA must be addressed through a formal performance improvement process. The final SLA must set out the applicable notice, corrective steps, review and, where necessary, contractual remedy or termination process.

5. DELIVERABLES

The service should provide at least the following tangible deliverables:

- A reliable full-time on-site IT support service from 08:00 to 16:00 for Section 1 and Section 2, backed by additional virtual and/or on-site expertise from the service provider where necessary.
- Reduced downtime for administrative staff, heads of department and educators.

- A stable and documented network, fibre, internet, switch and Wi-Fi environment.
- A more secure Wi-Fi solution that limits unauthorised learner access as far as practicable.
- Reliable technical support for the 35 fixed telephones/extensions and the existing 3CX environment.
- Efficient network support for staff printers within the scope of the existing Daisy contract.
- Reliable support for Action Timetable, d6, Google Admin/Google Workspace, WordPress and general office software.
- A complete and up-to-date IT asset register, purchase register, licence register and warranty register for the relevant scope.
- Regular preventive inspections and a documented maintenance programme.
- A backup, recovery and basic continuity plan for the school's applicable local data and core configurations.
- Monthly technical reporting and a usable ticket history.
- An annual statement of IT budget requirements delivered each June.
- A rolling three-year IT maintenance, upgrade and replacement plan.
- Full school control over administrator access, passwords, configurations, data and technical documentation.
- Clear cooperation and scope boundaries between Section 1 (CAT/IT classrooms) and Section 2 (administration/staff/network).
- A measurable SLA with agreed response, escalation and resolution times and ongoing performance measurement.
- A documented cybersecurity incident and remote access procedure.
- A documented IT onboarding and offboarding process for staff.
- Clear first-level support for school-approved, personally owned staff devices within the defined service scope.

6. KEY INFORMATION TO BE CONFIRMED BY THE SERVICE PROVIDER IN THE TENDER RESPONSE

To enable the school to evaluate proposals on a comparable basis, each tenderer should confirm at least the following in their response:

- Name, experience and skill level of the person proposed for the full-time on-site role, arrangements for absence/replacement, and the service provider's available second-/third-level, virtual and additional on-site support.
- Experience with 3CX, networks/switches/firewalls/Wi-Fi, Google Admin/Google Workspace, Windows/Microsoft 365, WordPress and general desktop support.
- Proposed ticket system, escalation process and reporting method.
- Proposed approach to limiting unauthorised learner access to staff Wi-Fi.
- Availability of second-/third-level technical expertise for specialised problems.
- Which services are covered by the fixed monthly fee and which items are regarded as additional/third-party costs.
- Any proposed exclusions must be expressly stated; silence on a core requirement may not subsequently be interpreted as an exclusion.
- Confirmation of whether the tenderer can provide data projector support, with a brief description of the scope and any separate costs, where applicable. Inability to provide this service will not in itself be an exclusion criterion.
- Confirmation that large photocopiers/multifunction copiers are not included in the tender price or service proposal.

- Confirmation that the tenderer will comply with the school's communication, approval, documentation and administrator access requirements.
- Confirmation that Department of Education Memo 416 of 2025 and the attached cabling/infrastructure specifications will be complied with in all relevant work.
- Confirmation that reasonable first-level technical support for school-approved, personally owned staff computers and laptops used for official school and teaching purposes falls within the proposed service scope. Any exclusions or additional costs applicable to such support must be clearly stated.
- Confirmation of whether the tenderer can offer an optional laptop rental/financing model for teaching staff or facilitate it through an appropriate third-party provider, as set out in the relevant annexure. Inability to provide this service will not in itself be an exclusion criterion.
- Completion of the proposed SLA response, escalation and resolution times in clause 2.15.1, with any relevant conditions or dependencies.
- Confirmation of the tenderer's proposed support for critical incidents outside normal on-site hours, including the escalation route and any additional costs.
- Confirmation that the tenderer can support the proposed cybersecurity incident, remote access, backup, recovery and continuity requirements, with any exclusions clearly stated.

Note: This needs analysis is intended as the technical basis for Section 2 of the school's IT support tender and must be read together with the final tender document, the CAT/IT needs analysis (Section 1), Department of Education Memo 416 of 2025 and the final SLA.

SECTION 3

OPTIONAL VALUE-ADDED SERVICE – LAPTOP RENTAL/FINANCING MODEL FOR TEACHING STAFF

Hoërskool Oos-Moot increasingly uses technology as an integral part of teaching and learning. Data projectors, visualisers, digital learning platforms, electronic administration, Microsoft 365, Google Workspace and other digital tools form part of educators' daily working environment.

A reliable laptop has consequently become an essential working tool for teaching staff.

Teaching staff are currently largely responsible for purchasing their own laptops. However, the cost of a suitable device can place a considerable financial burden on them, particularly young educators who have recently entered the profession.

As an **optional value-added component of this tender**, Hoërskool Oos-Moot would therefore like to establish whether the successful service provider can offer a laptop rental or financing model for staff or facilitate one through an appropriate third-party provider.

Proposed model

The school envisages a possible model under which:

- a staff member can rent or finance a suitable laptop over a period of approximately three (3) years;
- the individual staff member is personally responsible for the monthly payments;
- no rental or financing obligation is automatically assumed by the school;
- at the end of the term, the staff member may have the option to purchase the device for a predetermined or appropriate amount;
- a range of devices or specifications can be made available to meet different professional needs and budgets;
- the devices will be suitable for the school's existing technological environment and will work with, among other things, data projectors, visualisers, Microsoft 365, Google Workspace and other approved school systems; and
- appropriate warranty, repair, replacement and technical support options will be available throughout the term.

Information tenderers may provide

Tenderers able to offer such a service themselves or facilitate it through a third party are invited to submit a proposal including, where applicable, the following:

1. Available laptop models or specification categories.
2. Recommended minimum specifications for a teacher's daily use.
3. The proposed rental or financing term.
4. Estimated monthly cost per device or device class.
5. Deposit or credit requirements, if applicable.
6. The person or entity with whom the individual staff member will enter into the contract.
7. Ownership of the device during the contract period.
8. Conditions and costs for possible purchase of the device at the end of the term.
9. Warranty coverage.
10. Insurance against loss, theft or accidental damage, if available.
11. Repair and replacement arrangements if a device fails during the term.
12. Availability of a temporary/replacement device during repairs.
13. Technical support included in the rental/financing package.
14. Arrangements if a staff member retires or leaves Hoërskool Oos-Moot before the contract term is completed.
15. Possibility of early settlement or purchase.
16. Any administrative costs or other conditions applicable to the staff member.

Status of this request

This request forms an **optional, value-added component** of the tender.

A tenderer's ability or inability to offer this service will not in itself disqualify the tenderer from the core IT services tender.

This request places no financial obligation on Hoërskool Oos-Moot or its governing body. Any future scheme will be subject to applicable approval processes, legislation and the conclusion of suitable agreements between the parties concerned.

The school's purpose in making this request is to explore an affordable, accessible and sustainable way for teaching staff to obtain suitable technology that enables them to function effectively in the modern digital teaching environment.
