North27

Frederick Bremer School
AN EXCELLENT LOCAL SCHOOL IN THE HEART OF THE COMMUNITY

ICT Services Supplier

Request to Quote

December 2025 (Updated January 2026)

Executive Summary

Frederick Bremer School's managed service contract is due for renewal. Responses are sought under a single-stage process for a service provider to work with the school and their consultants (North27) to replace / extend the service.

Contract term and value. The school is seeking proposals for a **three-year term** (with an annual performance-related break clause) and an **expected total contract value up to £180,000 ex. VAT** across the term. Bidders may submit options for 3 + 1 with transparent year-on-year pricing.

Service model. Onsite L1–L2 support during term-time (42 weeks) complemented by remote L3–L4 engineering, with ad-hoc onsite L3–L4 days for planned works. See *Staffing & TUPE* and *SLA* for detail. This provision is all to support a directly employed L2+ technician and Business Manager who will manage the contract.

Vision. By the end of the 3 years the network should be primarily Google based, all core service e.g. MIS should be running in the cloud and all on prem either decommissioned or demoted to a secondary/backup role. This should then mean the support provision moves more to remote support.

Google Workspace is already embedded etc. so whilst the supplier should have some Google knowledge the main expertise required will be around Microsoft (to support and ultimately deprovision/decommission).

Strategic priorities (headline):

- Support the cloud initiative in a planned and cost effective way e.g. there should be no need for further server hardware. When something expires etc. it's an opportunity to replace it with a cloud alternative.
- Stabilise BAU operations and reduce ticket volume while improving first-time fix.
- Maintain and improve availability of core services (SIMS / FMS on-prem, Google Workspace, LGfL connectivity, telephony, printing, catering, AV).
- Support classroom AV refresh on a rolling plan aligned to teacher device strategy.
- Establish proactive **spares** policy (e.g. NAS / SAN drives, UPS batteries) and lifecycle management.
- Plan a 2027 review of **UPS and Disaster Recovery**, and options to move MIS to the cloud.

Background

Frederick Bremer School is a local authority–maintained **11–16 secondary school** with approximately **900 students**. The current campus opened in **2008** following a £20 million PFI build that merged two predecessor schools onto a single purpose-built site. The school forms part of **Waltham Forest's Building Schools for the Future (BSF)** programme and remains within a PFI management framework.

The school currently has a managed service provision provided by **Joskos Solutions** and has transitioned to a **hybrid managed service model**, combining onsite technical presence with external support and strategic oversight provided by **North27**. This model has stabilised operations and enabled structured improvements to infrastructure, classroom technology and user experience.

The PFI facilities management provider, Bouygues (ByUK) **now Equans**, continues to hold responsibility for core building systems – including passive cabling, CCTV, access control, and the Building Management System (BMS). The ICT managed service provider must coordinate effectively with PFI contractors and "own the issue" through to resolution where overlaps occur.

Further background information, including inspection reports and statutory details, is available via the **school website**: https://bremer.org.uk/ and the **Department for Education's Get-Information-About-Schools (GIAS)** service (formerly Edubase): https://www.get-information-schools.service.gov.uk/Establishments/Establishment/Details/103094 .

Technical Overview

Users and Devices

Frederick Bremer currently supports approximately **1,013 total users** (889 students and 124 staff). The end-user estate includes:

- **Windows 10:** One classroom set (around 30 devices) – currently under review for extension or replacement.
- **Windows 11:** Two classroom sets (around 60 devices) plus 20 staff machines.
- **Chromebooks:** Nine trolleys × 30 (270 devices) plus 10 spares and 10 SLT devices.
- **iPads (5th to 7th generation):** Around 20 to 30 units enrolled in Apple School Manager; iPadOS MDM required.
- **Staff laptops:** Around 100 not in daily use and 120 classroom-based in active use.
- **Music Macs:** 20 Apple iMacs used standalone with Logic Pro, managed via Apple School Manager.
- **Network utilisation:** Average switch load of approximately 29 per cent, leaving ample capacity for future expansion.
- **Students:** 889 active accounts.
- **Staff:** 124 active accounts.

Servers and Virtualisation

The school operates **two physical hosts** running **Microsoft Hyper-V**, which together host approximately **seven Windows Server 2012 virtual machines**, including SIMS and FMS.

Storage is provided by **two SAN units**, with additional **NAS capacity** used for archives and temporary data.

A **proactive spares policy** is required to hold replacement **NAS / SAN drives** and **UPS batteries**, ensuring minimal downtime in the event of hardware failure.

Backup systems perform **daily snapshots** and **weekly off-site replication**; the new provider will be expected to maintain, test, and document restore processes termly.

All servers should continue to receive **routine patching and OS updates**, with clear evidence logs maintained.

Migration planning should take account of end-of-support timelines for **Windows Server 2012**, with recommendations for phased upgrade or replacement.

Monitoring and alerting for server performance, disk utilisation, and hardware health should be in place and reviewed weekly.

Network Infrastructure

- The site is served by **one main server room** and **one secondary hub room**, each containing between **four and five switch stacks** (approximately four switches per stack).

- Current **switch utilisation averages around 29%**, providing substantial headroom for expansion, failure or future projects.

- Wireless coverage is delivered via approximately **36 Cisco Meraki access points**, including both indoor and outdoor units.

- The structured cabling and electrical infrastructure fall under the **PFI provider (Equans)**. Any faults or remedial works must be coordinated through PFI/FM.

- The network should be monitored weekly for utilisation, errors, switch health and spanning tree stability, with findings recorded and acted upon.

- Firewall, AV etc. alerts should be reviewed at least monthly, with recommendations shared in service review meetings.

- Accurate **network topology diagrams**, VLAN documentation and port-mapping records should be maintained and updated following every approved change.

Connectivity and Filtering

In support of Keeping children safe in education (KCSIE) 2025:

Internet connectivity is provided through **LGfL**, with a target bandwidth of **1 Gbps** to support curriculum, safeguarding and operational needs.

LGfL delivers the school's **web filtering, DNS protection and safeguarding services**, including monitoring and category-based blocking aligned to DfE requirements.

The ICT provider should monitor link performance, latency and utilisation, logging any outages or degradations and escalating to **LGfL NOC** as required.

Firewall management must include **monthly alert reviews**, tracking attempted access, blocked traffic and anomalies. This can be automated where possible and reviewed.

Resilience measures should be monitored and maintained, including correct failover behaviour, DHCP stability and VLAN routing.

Any changes to firewall rules, filtering categories or external access must follow the school's change-control process and be recorded for audit.

Maintaining security

In addition to the existing security obligations, the service provider must:

Support the school in achieving and maintaining Cyber Essentials (DfE-aligned) certification.

This includes:

- Helping to complete a full readiness assessment against Cyber Essentials controls.
- Identifying gaps in current practice, including device compliance, patching, firewall rules, MFA, access policies, and secure configuration.
- Providing clear remediation actions, with timelines, costs (if any), and technical guidance.
- Assisting with technical implementation of required changes as part of normal service delivery.
- Preparing evidence for the certification questionnaire and supporting the school through submission and renewal.
- **Conduct an annual cyber security audit** to verify ongoing compliance with Cyber Essentials and DfE cyber security standards, including a written report with prioritised risks and recommendations.
- **Advise on alignment with DfE and NCSC cyber security expectations**, including incident response, password policy, backup resilience, and staff awareness.

Identity, Email and Productivity

The school operates a **hybrid identity environment** using **Microsoft Active Directory** and **Azure AD**, alongside **Google Workspace** for email and collaboration.

The managed service provider must maintain AD hygiene, including OU structure, Group Policy Objects, password policies and privileged access control.

MFA should be enforced where appropriate and regularly reviewed for staff, admin accounts and remote access pathways.

Google Workspace administration includes account provisioning, Groups management, OU structure, security controls and alignment with the school's safeguarding policies.

SSO integration between Microsoft, Google and third-party services should be maintained and improved where possible.

Microsoft Office (desktop) and Google Workspace (mail) continue to operate in tandem; the provider should ensure licensing compliance and maintain optimal configurations.

The managed service should support password reset procedures, mobile device access policies and identity lifecycle management for starters, leavers and role changes.

Helpdesk and Monitoring

- The school (internally) currently uses **Spiceworks** as the service desk platform; the provider (perhaps through another system) must manage categories, priorities, SLA timers, reporting and user communication.

- Bidders may propose an alternative service desk platform if it offers clearer reporting, better automation or improved user experience.

- Typical baseline ticket volume is around **150 ± 30 tickets per month**; the provider should aim to reduce this through first-time fix, automation and problem-management.

- All incidents should follow L1–L4 escalation paths, with clear communication to staff and leadership during major issues.

- The provider must maintain a **knowledge base** to support staff self-service and improve consistency of responses.

- **Senso Cloud** is used for classroom management and safeguarding; it must be monitored and supported as part of the core service.

- Device monitoring should capture endpoint health, AV/EDR compliance, disk utilisation and update status, with weekly review and action.

- Alerts from servers, switches, wireless controllers, firewall and backup systems must be reviewed daily, with P1 issues escalated immediately.

- Trends and recurring issues should be analysed and reported in monthly service reviews, with recommendations for reduction and prevention.

PFI / Building Systems (Equans)

The site's **passive cabling, CCTV, access control systems and Building Management System (BMS)** fall under the responsibility of the PFI provider .

Any cabling faults, power issues, or infrastructure-related concerns must be escalated to the PFI/FM team, with the ICT provider tracking progress and ensuring issues are driven to completion.

The ICT provider must "**own the issue**" where problems span ICT and PFI boundaries, ensuring the school does not become the coordinator between suppliers.

The provider is expected to maintain a clear **responsibilities matrix** showing ICT, PFI, on-site teams and third-party vendors, ensuring the school has a single, simple view of accountability.

Any planned ICT works impacting PFI-controlled areas must follow the appropriate permit and approval processes through FM.

Coordination should be maintained during term time and school events to minimise disruption, particularly for AV upgrades, cabling changes or server room work involving PFI-controlled spaces.

Compliance and Safety

- All onsite ICT staff must hold a current **Enhanced DBS** issued within the last three years and must complete the school's safeguarding induction before undertaking any work on site.

- The provider must ensure that all staff follow the school's **Safeguarding**, **E-Safety**, **Acceptable Use** and **Health & Safety** policies at all times.

- Any contractor or third-party engineer visiting the site must be supervised in line with the school's safeguarding procedures unless they hold appropriate DBS clearance.

- The provider is responsible for maintaining accurate training records for its staff, including safeguarding, data protection, H&S awareness, and any relevant technical certifications.

- All ICT work must comply with the school's **risk assessment** requirements, especially when carrying out activities involving ladders, AV mounting, power isolation, or work within PFI-controlled spaces.

- Data handling must follow UK GDPR principles, with secure storage, access control and data minimisation observed at all times.

- Any safeguarding or data-related incident must be reported to school leadership immediately and followed through to full resolution with documented actions.

- The provider must support the school in maintaining secure, compliant systems used by staff and students, including monitoring for unsafe behaviour, inappropriate access or device misuse (e.g. via Senso Cloud).

Outstanding Items

- **Proactive spares** (NAS/SAN drives and UPS batteries) should be established as standard consumables and added to the lifecycle plan.

- A review is required of the **teacher device strategy** to determine whether each member of staff should have their own device or continue using classroom-based equipment.

- **Windows 10 devices** need a decision on extension, replacement, or conversion to a supported platform before end-of-life.

- **MIS cloud migration** (Next Gen or Arbor etc.) should be considered as part of the 2027 strategic review.

- **Gifted laptops** to be assessed for conversion to **Chromebooks** (where licensing allows) to simplify management.

- Ensure all switch utilisation, server capacity and wireless coverage findings are correctly reflected in the updated technical documentation (e.g. 29 per cent utilisation figure).

Requirements

Scope of Managed Service and Requirements

The managed service must provide a reliable, secure and forward-looking ICT environment that supports teaching, learning and school operations. Requirements include:

- The school prefers suppliers that are listed on a recognised UK public-sector framework (e.g. CCS RM6103 or Everything ICT) or can demonstrate equivalent compliance with public-sector procurement standards.
- Stable day-to-day ICT operations with clear SLAs, fast response times and a reduction in ticket volumes over time.
- A proactive approach to maintenance, monitoring and lifecycle planning across all infrastructure areas.
- Effective coordination with all third-party suppliers, with the provider "owning the issue" end-to-end.
- Support for the school's mixed environment of Windows, Chromebooks, iPads and Mac devices.
- Compliance with safeguarding, data protection (UK GDPR), e-safety and H&S expectations for all onsite and remote staff.
- Accurate documentation, including inventories, network diagrams, backup reports, risk registers and change logs.
- Forward planning for 2027, including evaluation of MIS cloud migration options and a full review of UPS and Disaster Recovery arrangements.
- Delivery of teacher-facing and classroom-focused support to maximise reliability and minimise lesson disruption.
- Support for secure and responsible use of AI tools (e.g. ChatGPT) aligned with safeguarding expectations.

- Flexibility to propose improvements to infrastructure, licensing, device strategy and workflow efficiency.

Service Desk & User Support

- Full management of Spiceworks (or proposed alternative) with SLAs, escalation paths and first-time fix focus.
- Targeted reduction in ticket volume through automation and root-cause resolution.
- Clear communication with staff, including outage updates and planned maintenance notifications.

Systems Administration

- Management of Microsoft AD, Azure AD and Google Workspace, including MFA and password policies.
- Windows 11 image creation and rollout, with Windows 10 lifecycle and replacement planning.
- Patch management, AV/EDR compliance monitoring and endpoint encryption where appropriate.

Backup, DR & Continuity

- Daily backup checks and termly restore tests (file, email and full system).
- Maintenance of DR documentation and continuity plans.
- Full 2027 review of UPS estate, DR plan and options for cloud migration of core services including MIS.

Network & Wireless

- Weekly monitoring of switches and wireless performance; monthly firewall log review.
- Capacity planning, error tracking and utilisation reports (including the 29 per cent baseline utilisation).

- Coordination with PFI/FM for passive cabling and electrical works (e.g. West Wing earthing).

AV & Classroom Technology

- Rolling AV maintenance (projectors, panels, bulbs, mounts, shutdown routines).
- Alignment of AV refresh cycles with the staff-device strategy.
- Assessment of gifted laptops for conversion to Chromebooks where appropriate.

Third-Party Coordination

Single point of accountability for:

- MIS: SIMS & FMS (via SBS),
- Telephony: The Comms Guys,
- Print Management: PaperCut,
- Cashless Catering: Cunninghams iPay/Impact,
- Backup: Jcloud (Joskos),
- LGfL inc. helping to make the most of the bundled license e.g. AV and Meraki
- Microsoft,
- Google (North27 can help here if needed)

Asset Management & Lifecycle

- Maintenance of full hardware, software and licensing inventories.
- WEEE-compliant disposals with certificates of data destruction.
- Proactive spares: SAN/NAS drives, UPS batteries, AV consumables and rapid-swap devices.

Governance & Reporting

- Monthly KPI reports; termly summaries; annual full service review.

- Production of a RACII matrix within the first month of contract start.

Strategic Planning

- Work with North27 to align infrastructure development with curriculum and operational needs.
- Prepare for 2027 strategic reviews: UPS and DR plan, cloud migration, and device refresh strategy.
- Support sustainable purchasing and configuration practices to reduce energy consumption and waste.

Activity	Frequency (Minimum)	Notes
Helpdesk		
Maintain and monitor	Daily	The helpdesk/service desk software must be used as the central management tool for SLAs, workloads and trends. Every support interaction must be logged so performance, safeguarding issues and recurring problems can be monitored and addressed. The provider should work to reduce ticket volume (baseline ~150 ±30 per month) by improving first-time fix, automation and problem management, with trends reported in the monthly KPI pack.
General		
Keep documentation up-to-date	As necessary	Including: recovery passwords, network topology, hardware inventory, software inventory, licences, DR documentation, backup procedures and the responsibilities/RACII matrix. Documentation must reflect current systems and changes.
Send client log of work performed	Monthly	Format and detail to be agreed. Typically included in the monthly KPI report and service review meeting.
System maintenance		
Check backups are running properly	Daily	Backup jobs, replication and snapshots must be checked and issues resolved. Errors on open SQL databases (e.g. MIS, finance) must not be ignored and must be remediated.

Perform backup test	Termly	A full restore test including file, email and Bare Metal Restore (BMR). Evidence must be recorded and reported.
Monitor and maintain server uptime	Constantly	Automated tools must monitor availability of on-prem and cloud services, with alerts investigated promptly.
Install software patches, service packs and other updates	As necessary	Updates must be tested where appropriate and deployed in a timely manner. Patch compliance reported monthly.
Install software upgrades	As necessary	Major upgrades and those with costs require approval by the client before deployment.
Monitor server event logs for potential problems	Daily	Warning and error events must be investigated and remediated with root-cause analysis where appropriate.
Monitor status and availability of cloud services	Constantly	Automated alerting must be used for key cloud services including MIS, Google Workspace, telephony, safeguarding systems and LGfL..
Monitor disk health and available disk space for NAS/SAN and servers	Daily	Check disk failures, capacity thresholds and SAN/NAS status. Maintain proactive spares such as NAS/SAN drives and UPS batteries.
Replication Health	Daily	Check virtual machine replication, Hyper-V replica status and synchronisation.
Perform system and server reboots	As necessary	Reboots should be planned out-of-hours or agreed times to avoid lesson disruption.
General server maintenance	As necessary	Routine housekeeping including performance optimisation, with work carried out during agreed windows.

Let client know of any potential issues	As necessary	Examples include low disk space, failing components, deteriorating broadband speed or expiring warranties.
Create, remove and maintain staff user accounts and permissions	As necessary	Includes starters, leavers, role changes and permission adjustments across AD, Azure AD, Google Workspace and MIS-linked accounts.
Manage Active Directory (AD)	As necessary	Includes GPO management, OU hygiene, MFA policy alignment and disabling stale accounts.
Assist users with support queries	As necessary	Examples: VPN access, shared file locations, Google/Microsoft sign-in issues.
Manage Google Workspace	As necessary	Ensure SSO works, manage OUs, Groups, permissions, mailbox issues and security controls.
Fixing problems		
Disaster recovery of core systems	As necessary	In major incidents (e.g. server failure, ransomware), restore services following the DR plan. DR plan must be maintained and reviewed annually.
Fix user errors / mistakes	As necessary	Examples: accidental deletion, password resets, incorrect configurations.
Raise support requests with third-party providers	As necessary	Supplier must “own the issue” to resolution.
Managing networks		
Maintain internet connection	Constantly	Monitor LGfL link performance, availability, latency and escalate issues promptly.
Monitor logs	Weekly	Review system logs across switches, servers, wireless controllers, firewalls and key applications.

Monitor network capacity and performance	Weekly	Identify where capacity approaches limits (current baseline ~29% utilisation). Recommend improvements.
Maintaining security		
Monitor firewall logs	Monthly	Identify suspicious activity and ensure rules remain aligned to security policies.
Check status of security software updates inc. Anti-Virus	As necessary	Ensure endpoint protection, web filtering clients and EDR agents are fully up to date.
Investigate any suspicious activity or unexpected software behaviour	As necessary	Investigate events such as malware, ransomware, hacking attempts or unauthorised access attempts.
Manage file and folder permissions	As necessary	Manage permissions across on-prem, Microsoft 365 and Google Workspace environments.
Enforce password policies	As necessary	Ensure password policy and MFA settings align with safeguarding and security expectations.
Managing apps and cloud services		
Software & imaging	As necessary	Includes WDS/MDT drivers, Windows 11 images, application packaging and deployment.
Create, manage and remove accounts/mailboxes	As necessary	Email accounts, permissions, mailbox size changes and SIMS-linked accounts.
Managing mobile devices		
Mobile device management (MDM) for iPad devices	As necessary	App rollout, OS updates, configuration changes, ASM enrolment and safeguarding profiles.
Managing projectors		
Manage to prolong life and maximise uptime	As necessary	Clean/check equipment, check shutdown routines, replace bulbs/consumables, prepare AV for events.

Equipment disposal		
Manage equipment disposal	As necessary	All equipment must be disposed of in line with WEEE requirements and UK GDPR, with data wiped to NCSC-aligned standards and certificates provided.

In addition the service provider/team should seek to support the school with its aims, as is fair and reasonable within the amount of time available. Occasionally support out-of-hours e.g. exam results, open evenings; new user induction training, basic Internet and office application training e.g. saving, printing.

Work with third party suppliers/support providers, identify upgrades/replacements and share.

Staffing

Note: Levels as defined by ITIL.

The managed service will be delivered through a dedicated onsite technician (L1–L2) available for 42 weeks per year to provide day-to-day support, classroom assistance, device maintenance, AV checks and escalation where required.

This is supported by a remote senior engineer (L3–L4) responsible for advanced troubleshooting, configuration, escalated incident management and change control, with critical onsite response available within one hour when needed. With remaining time towards wider cloud migration.

The supplier must also provide a minimum of 10 onsite L3–L4 engineering days per year for planned improvements such as AV refresh, lifecycle tasks, network optimisation and server maintenance. Clear cover arrangements for sickness, leave and training must ensure uninterrupted onsite and remote support, with additional support provided for key events such as exam days, open evenings and critical maintenance windows.

North27 will remain involved for oversight where required. TUPE context applies: an onsite technician previously transferred to the school; bidders must confirm their TUPE assumptions during clarification. All onsite staff must hold a current Enhanced DBS and complete the school’s safeguarding induction before commencing work.

All other non BAU work will be run as projects, with defined budgets, outcomes, targets and signoff requirements.

Timescale & Process

Quotations will be sought in the following timescale:

The procurement will follow the revised timescale below. These dates ensure adequate internal review time for the school and a fair and compliant process for suppliers.

• Friday 19th December2025 – RfQ issued
• 19th December - 9th January – Clarifications window (Q&A log published twice weekly)

• **Monday 19th January 2026, 12:00 (midday) – Submission deadline**
• 19th-20th January - Compliance checking and initial scoring
• 26th January - Shortlisted supplier interviews (preferably in person at the school)
• 27th-29th January - Moderation and reference checks
• 30th January – Preferred bidder notice (intention to award)

• 30th January - 8th February – Standstill period (10 calendar days)
• 2nd February - Incumbent provides ELI to preferred bidder (if required)
• 11th February - Contract Award
• Monday 2nd March 2026 – Go-live / service transfer

The quote should ideally follow the format of the evaluation criteria and reference the content and appendices within this document.

The final quotation should submitted as a pdf, with all costs in a supporting spreadsheet and emailed to: Shermaine Lewis [s.lewis@bremer.waltham.sch.uk] and Andrew Howden [andrew.howden@north27.co.uk] no later than the deadline detailed above. Responses will not be reviewed until after the deadline.

Quality Assurance

The supplier must operate a clear and robust Quality Assurance framework to ensure that all services are delivered consistently, safely and to the required standard. This includes maintaining accurate documentation, following agreed processes, and ensuring staff skills and compliance remain current. The supplier will be expected to demonstrate continuous improvement throughout the contract, using evidence from monitoring, reporting and service reviews.

Quality assurance measures must include:

• Consistent adherence to agreed SLAs, KPIs and escalation procedures
• Accurate and up-to-date documentation covering network diagrams, inventories, backup logs, DR procedures, security settings and change control

- Monthly KPI reporting including ticket volumes, first-time fix rates, patch compliance, AV/EDR status, backup performance and service trends
- Termly service review meetings to assess performance, progress against the roadmap, open risks and agreed improvement actions
- An annual full-service audit covering infrastructure health, security posture, backup and DR integrity, device lifecycle, licensing, user experience and support performance
- Processes that ensure safeguarding, data protection (UK GDPR) and Health & Safety requirements are followed at all times
- Quality checks on all engineering work, including peer review for changes or configurations that carry elevated risk
- Use of root-cause analysis for recurring incidents, feeding outcomes into the improvement plan
- Evidence of staff training, certification and background checks, including Enhanced DBS for onsite personnel
- A commitment to continuous improvement, with recommendations for efficiency, security, sustainability and user experience

The supplier will also be required to submit a RACII responsibilities matrix within the first month of the contract to confirm roles, responsibilities and boundaries across the School, the Supplier and third-party providers.

Health and Safety

The supplier must ensure that all work carried out on school premises complies fully with relevant Health and Safety legislation, the school's own H&S policies, and industry best practice. All onsite staff must follow the school's procedures at all times and ensure that risks are managed proactively, particularly in teaching environments and areas accessed by students.

Health and Safety expectations include:

- All onsite personnel must hold a current Enhanced DBS and complete the school's safeguarding and H&S induction before commencing work.
- Risk assessments must be completed for activities including AV mounting, ladder use, cabling, electrical work, server room activity, and work in PFI-controlled areas.
- All ICT work must be undertaken with due regard for the safety of students, staff and visitors, ensuring tools, equipment and cabling do not create hazards.
- Any work requiring power isolation, ceiling access, or changes to fixed installations must be coordinated with the PFI/FM provider and follow their permit-to-work processes.
- The supplier must ensure that electrical and network equipment is safely installed, maintained and operated, with faults (e.g. earthing issues in the West Wing) escalated promptly and followed through to resolution.
- Hazardous activities must only be carried out by competent and appropriately trained staff.

- Portable electrical equipment used by the supplier must be safe, regularly inspected, and compliant with the school's electrical safety policy.
- The supplier must report any Health and Safety incidents, near misses or unsafe conditions immediately to the school's nominated contact and document actions taken.
- Waste electrical and electronic equipment (WEEE) must be handled and disposed of in a safe, compliant manner with environmental and data-wiping standards met.
- All engineering work must be planned to minimise disruption and risk during the school day, with intrusive work arranged outside teaching hours where practicable.

The supplier must maintain evidence of risk assessments, staff training, incident logs and safety controls, and make these available to the school on request.

Intellectual Property

All intellectual property ("IP") arising from the delivery of this service, including documentation, configurations, scripts, templates, images, processes or other materials created specifically for Frederick Bremer School, shall belong exclusively to the School. The supplier shall grant the School a perpetual, irrevocable, royalty-free licence to use, modify and distribute any such materials for the purposes of operating, maintaining or developing its ICT environment.

Where the supplier uses pre-existing materials developed independently of this contract (including proprietary scripts, tools or documentation), ownership of those materials shall remain with the supplier; however, the supplier must grant the School a non-exclusive, royalty-free licence to use such materials for the duration of the contract and any transition period.

The supplier must not restrict, obstruct or withhold information, passwords, documentation or configurations that would prevent the School or its appointed representatives from operating or supporting the ICT environment. Source data, administrative credentials, system configurations and service documentation must be handed over in full upon request, during the contract and at the point of exit.

Any third-party intellectual property used in the service must be appropriately licensed, and the supplier shall be responsible for ensuring compliance with licence terms. The School shall remain the Data Controller for all data created or held within its systems, regardless of where it is processed or stored.

On termination or expiry of the contract, all materials, documentation, configurations, credentials and data must be securely transferred to the School or its nominated successor, and the supplier must provide written confirmation that no copies of school-owned IP or data are retained, except where retention is required by law.

Language

All documentation, correspondence, training, and support shall be in English.

Warranty

The supplier must ensure that all hardware and software provided, installed or supported under this contract is covered by an appropriate manufacturer's warranty or equivalent support provision. The supplier is responsible for managing warranty claims on behalf of the School, including logging, tracking and coordinating repairs or replacements directly with the manufacturer or authorised service provider.

Where equipment is supplied by the School, the supplier must maintain accurate warranty records and notify the School in advance of any equipment approaching the end of its warranty period. The supplier must also advise on extended warranties, lifecycle planning and replacement options where appropriate.

All warranty repairs must be completed in a timely manner, with the supplier providing suitable loan or replacement equipment where necessary to minimise disruption to teaching and learning. This includes ensuring that loan devices are appropriately configured, secure and fit for purpose.

Any replacement components or devices installed under warranty must be recorded in the School's asset register and comply with relevant standards for compatibility, performance and energy efficiency.

The supplier must ensure that warranty conditions are adhered to at all times, including correct installation, environmental requirements, firmware updates and maintenance practices. Misconfiguration, unauthorised repairs or failure to follow recommended procedures must not invalidate warranties.

Where the supplier provides any bespoke configuration, documentation, scripts or solutions, the supplier warrants that such work will be free from defects and will function as intended for a minimum period of 90 days from delivery. Defects identified within this period must be remedied at no additional cost to the School.

Conduct of procurement procedure

These instructions and conditions are designed to ensure that all potential suppliers are given equal and fair consideration. It is therefore important that all requested information is provided in the format and order specified. Further negotiations are not permitted as part of this process.

Nothing contained within or outside of this quote shall be taken as constituting a contract or agreement between Frederick Bremer School and any other party.

While every effort has been made to ensure that this document accurately reflects the School's requirements, suppliers must form their own conclusions regarding the methods, resources and materials needed to meet these requirements. The School does not accept responsibility for any estimates made by suppliers in relation to the resources required, or for any assumptions drawn from pre-contract discussions.

Statements by the School regarding the future process or timing of the procurement represent the School's current intentions only. The School reserves the right to vary the procurement procedure at any time by notice in writing, including the right to terminate the process entirely.

Frederick Bremer School is not committed to any course of action as a result of issuing this quote. The School may exclude any supplier that does not comply with these instructions and conditions, and may choose not to accept any response. The School does not commit to accepting the lowest price or any best-and-final offer.

Frederick Bremer School is committed to upholding the Seven Principles of Public Life (Nolan Committee) and expects all participating suppliers to honour and support this commitment. More information on the principles is available at: https://www.gov.uk/government/publications/the-7-principles-of-public-life.

Incomplete Quote

Quotes may not be considered if the complete information is not provided.

Receipt of quotes

Quotes must be submitted electronically in PDF format, together with a separate pricing schedule, by the stated deadline. Submissions must be sent to the named School contact(s) as specified in this document. Please ensure that all required attachments, supporting evidence and declarations are included.

Late submissions cannot be accepted under any circumstances. It is the responsibility of the supplier to ensure that the quote is submitted on time and that all documents are readable and complete. The School cannot accept responsibility for transmission delays or technical issues encountered by the supplier.

All quotes will be opened only after the submission deadline. Quotes will be treated in confidence and evaluated in accordance with the published criteria. Any attempt to influence the procurement process or make unauthorised contact with School staff may result in disqualification.

The supplier must ensure that the submission clearly states the name of the organisation, the contact details of the authorised representative, and the validity period of the quote (which must be no less than 90 days from the submission deadline).

By submitting a response, the supplier confirms acceptance of the instructions and conditions of this RfQ and acknowledges that the School is not bound to accept the lowest price or any proposal submitted.

Non-collusion and inducements

You shall ensure that your quote is bona fide, aimed at obtaining the award of a contract on the grounds of best value for money to Frederick Bremer. This means that there will not be any form of collusion with any other potential supplier.

You shall not at any stage do any of the following acts:

- communicate to any other person involved in the quoting the amount or approximate amount of your quote
- enter into any agreement or arrangement with another person (or a person on behalf of that other person) so that the person shall refrain from participating in any part of the procurement process
- offer, pay, give or agree to pay or give (nor solicit, receive or accept) consideration directly or indirectly to any person for having done or for doing in relation to another person's participation in the procurement

Breach of this clause will entitle Frederick Bremer to disqualify a quotation and may constitute a criminal offence. In this paragraph, the word "person" includes any person, body or association, corporate or otherwise, and "any agreement or arrangement" includes any such transaction, formal or informal and whether legally binding or otherwise.

Confidentiality

Frederick Bremer and the bidding suppliers' organisation agree that each shall keep confidential all information, whether written or oral: concerning the business and affairs of the other party (and the other party's suppliers, service providers, agents and representatives) and all other information which it is notified is confidential from, or on behalf of, the other party which it receives or obtains as a result of its involvement in the procurement. There may be some information which is in, or falls into, the public domain which would not breach this clause, and to comply with all reasonable requests of the other party in relation to such information (including, where appropriate, entry into appropriate confidentiality undertakings). Failure by you to comply with this clause will entitle Frederick Bremer to disqualify your quote.

Offers and acceptance

Frederick Bremer will send a letter to award the contract to the successful service supplier. Frederick Bremer will notify each unsuccessful bidder as soon as is reasonably practicable.

Please note that the school:

- is not bound to accept the lowest price
- reserves the right to accept any part of the response as it may deem appropriate

Applicants must submit a quote that is compliant with all the requirements of this request to quote.

Frederick Bremer accepts no liability to pay any costs and expenses which may be incurred by, or on behalf of, the supplier's organisation and your consortium members in preparing for this request to quote.

Clarifications

Clarifications should be emailed to Andrew Howden [andrew.howden@north27.co.uk]. Responses will be anonymised and shared with all where appropriate, in an open and transparent manner via this Google Drive link: Frederick Bremer MSP RfQ - December 2025.

Evaluation criteria

The process will be conducted in a way that helps to ensure that all are evaluated fairly in order to establish the best value and most appropriate solution for Frederick Bremer.

Criteria	Weighting %	Test Area
Educational transformation	5	Meets the School's requirements and supports educational improvement, reliable classroom delivery, staff device strategy, and future technology planning (e.g. Windows 11, AV refresh, MIS cloud roadmap).
Value for money	30	Transparent pricing methodology, fairness of cost, whole-life value, efficient use of resources, proactive spares model, and demonstrable value over contract term.
Service transfer	10	Ability to manage a smooth transfer into service, including onboarding, documentation handover, access credential management, and transition from incumbent or existing arrangements without service disruption.
Contract management	5	Structure and processes for managing the service, quality of management information, meeting governance requirements, and ability to deliver monthly KPIs, termly reviews, and annual audits.
Risk management	10	Identification and management of risks including PFI dependencies, infrastructure health, DR/UPS 2027 review, licensing, end-of-life hardware, and operational continuity.
Data management	5	Provision of data protection, security controls, compliance with UK GDPR and safeguarding requirements, secure handling of school data, backup integrity, DR planning, and support for Senso Cloud.
Technical compliance	15	Ability to meet the School's technical requirements.
Environmentally sustainable	5	Evidence of sustainable practices including lifecycle planning, energy-efficient configuration,

		WEEE-compliant disposal, and minimising environmental impact of service delivery.
Quality	15	Quality assurance processes including continual improvement, incident/problem management, documentation standards, and evidence of robust operational procedures.

Appendices

Appendix 1: SLA
Appendix 2: Example Services Contract
Appendix 3: Inventory [Available on request]
Appendix 4: Responsibilities matrix
Appendix 5: Safeguarding

- Safeguarding Policy
- E Safety Policy

Appendix 6: Map [Available on request]