Request for Proposal
for IT / Cyber Security Support Partner

1 Background and Context

Sage Advocacy is the National Advocacy Service for Older People. It works to ensure that people have easy access to independent support and advocacy services in all settings: homes, day centres, respite facilities, congregated care settings / nursing homes, hospitals, hostels, hospices and in the process of transition between them. Since it was established in 2014, with the support of the HSE and The Atlantic Philanthropies, it has built a strong reputation for independence of thought and action and is a 'go to' service in relation to issues of capacity and decision making.

Sage provided information, support and advocacy services to over 11,000 people in 2024 and our work on behalf of clients is independent of family, service provider and systems interests. Our services are free of charge and confidential. Sage Advocacy ensures that a person's voice is heard, that their wishes are taken into account and that they are assisted, in whatever ways necessary, to be involved in decisions that affect them.

The motto of Sage Advocacy is 'Nothing about you / without you'. Sage Advocacy's approach is to collaborate where possible and to challenge where necessary. There is a strong focus on achieving social impact by addressing underlying systemic issues raised through individual case work. Our work is guided by Quality Standards for Support & Advocacy Work With Older People, a Case Management Group and by the Guiding Principles of the Assisted Decision Making (Capacity) Acts.

Responsibility for the overall development and governance of the service rests with the Board of trustees of Sage Advocacy clg.

2 Objective

Sage is looking for a strategic IT support partner to enhance our IT infrastructure, security, and overall management. The partner will implement, manage and maintain our Windows desktop and laptop devices and Microsoft cloud platform, providing proactive support and act as a trusted advisor on technology trends, security and cost management.

As part of this service, the chosen IT support partner will be expected to:

1. **Ensure the implementation of robust infrastructure and security measures** within Microsoft 365, the internal network and across all devices to enhance the protection of the Organisation's data.
2. **Regularly support and maintain these components proactively**, providing detailed monthly reports showing key security and service KPIs as well as highlighting activities performed during the period.
3. **Offer comprehensive support to end-users** by establishing an efficient IT help desk to address problem reports and user inquiries on a day-to-day basis.
4. **Act as a strategic partner and advisor to the Organisation**, proactively informing Sage about current technology trends and emerging threats, recommending actions and identifying cost management opportunities to help us minimise costs while remaining at the forefront of industry best practices.
5. **Maintain the Organisation's IT equipment** to ensure operational efficiency and reliability.

3 Current Environment

3.1 Technology

Sage operates a technology environment that is primarily based on:

- Microsoft 365
- Windows Devices (Primarily Lenovo laptops, plus several desktop PCs in the office)
- End-User Software Applications (Primarily MS Office apps)
- Samsung Phones (All owned by the Organisation)

3.2 Staff

- There are currently 60 full-time employees. Approximately 13 of these staff members are based in the 'National Office' on Ormond Quay (but also work remotely). The remaining staff are 'advocates' who all work remotely and are based throughout the country.

- The Organisation is likely to grow to 100 staff members over the next 3 years. Most of the new joiners will be advocates who will work remotely.

3.3 Physical Office

- Sage's main 'National Office' is on the ground floor of 24 – 26 Ormond Quay, Dublin 7. This office is only accessible to Sage staff – It is not open to the public. The Organisation is planning to relocate to another premises over the coming months. The move is not yet agreed but if it does proceed, it is likely to be within the Dublin City Centre area.

- There are approximately 13 desks within the office. Each desk is set up with:

  - A desktop PC.

  - A monitor.

  - A keyboard.

  - A mouse.

  - A desk phone.

- There is one meeting room in the office. In this room, there is a shared laptop which is connected via USB to a Logitech Group video conferencing system.

- There is also an MFP printer/scanner in the office. It is accessible to desktop PCs and laptops through the wired and wireless networks. **NOTE**: The device is managed by a separate 3rd party so is not within the scope of this RFP.

- There is also a VoIP phone system installed in the office. While there are phones on every desk, only a subset of staff use them anymore. Most staff just use their mobile phones. **NOTE**: The VoIP service is managed by a separate 3rd party so is not within the scope of this RFP.

- There are wired and wireless networks within the office.
    - The wired network is used to connect the printer, desk phones, desktop PCs, and the meeting room laptop to the network and internet.
    - There is one wireless network in the office. Staff use a static WiFi password to connect their work laptops to this WiFi network so they can access the local network and internet.
- All of the main networking equipment is in a comms cabinet, which is located in a store room within the main office. This cabinet includes the following:
    - Virgin Media broadband router - This enters the office behind the comms cabinet. The broadband contract is directly between Sage and Virgin Media.
    - There is a connection between the Virgin Media router and the office firewall. The firewall is a SonicWall (DELL) SOHO Wireless-N device (purchased in June 2017).
    - This firewall is connected to two switches:
        - The first switch is an LG 100mb switch. This is used by the phone system (mentioned earlier).
        - The second switch is a newer DrayTec 1gb switch.
        - As mentioned earlier, there is a phone on each desk, but only about 50% of these are used. On desks where the desk phone is still used, the desktop PC's are daisy-chained through the phone to the wired network and routed through to the older LG switch. On desks where the phone is no longer used, the desktop PC's are connected to the wired network directly and patched through to the newer DrayTec switch.
    - This firewall device also provides the office wireless network mentioned earlier. There are no other Wireless Access Points in the office.
    - Within the cabinet, there is also a Hikvision CCTV DVR device, which was upgraded within the last year. This is a standalone unit and is not connected to the LAN or the internet. It records footage from a security camera located outside / above the front door. On a desk between the front door and store room, there is a monitor showing the live feed from the camera. This enables staff to verify the identity of anyone at the front door. The monitor is connected to the PVR through a long HDMI cable. A wireless mouse is also on the desk, enabling staff to operate the live feed from the desk. NOTE: Technical support of this **is** included within the scope of services to be provided by the selected IT MSP, as this system is currently managed by our current IT support provider.

3.4 End User Devices

NOTE: The Organisation will continue to purchase / replace laptops, desktops, and phones directly. The purchase of this equipment is **NOT** within the scope of this RFP. However, ongoing support of this equipment **IS** within scope.

Corporate Laptops:

- All staff have a corporate-owned laptop. They are primarily Lenovo devices. One staff member uses her own Mac.
- The current age of our laptops ranges from 0-5 years.
- The devices are running a mix of Windows 10 or Windows 11.

Corporate Desktops:

- There is a desktop PC on or under each desk in the office.
- These 13 desktop PCs are Lenovo ThinkCentre M70s (purchased between October 2022 and October 2023). They each have a Core i5-10500 processor, 16GB of RAM, 512GB SSDs, and all run Windows 10 Pro.
- Any staff member can log into a desktop PC once a local profile has been configured on the device for them and a local PIN has been configured by them.
- **NOTE:** Every staff member has a laptop. Therefore, if the ongoing use of these desktop PCs results in significant additional support costs or adds unnecessary complexity to your proposed support service, Sage is open to reviewing the need for these desktop PCs in the future.

Corporate Phones:

- All staff have a corporate-owned phone – They are primarily Samsung A15 devices.

Non-Corporate Devices:

- There are currently no technical controls in place to prevent M365 data from being accessed on a non-corporate device.

3.5 Microsoft 365

- **Microsoft 365 users / licenses**: We currently use in the region of 100 user licenses, due to the number of staff members, board members, advisors, volunteers, and committee members. The Organisation will continue to purchase Microsoft 365 licenses directly (as Microsoft provides preferential pricing to charities). Therefore, the purchase of Microsoft 365 licenses is **NOT** within the scope of this RFP.

- **Microsoft Teams**: Widely used for meeting and collaborating.

- **Microsoft SharePoint and OneDrive:** Used for document storage, collaboration and file sharing.

3.6 Security-Related Tools

1. **Endpoint Protection:** Webroot is installed on all laptops and desktops. We recently engaged an external party to perform a high-level security review of a small sample of the laptops, and several recommendations emerged. This includes the need for centralised monitoring and management of the laptops, desktops, and phones (e.g. via Microsoft Intune), to ensure there is consistency in the security configuration of the devices.

2. **Microsoft 365**: We recently engaged an external party to perform a security assessment of this environment, and several recommendations emerged.

3. **Backups:** Our IT MSP recently migrated from an AWS-based backup of our M365 environment to Microsoft 365 Backup Services.

4 The Requirement

Sage is in search of a strategic technology partner capable of providing expert guidance and leadership to help us improve our security posture and align to industry best practice.

The selected IT managed service provider will assume the role of Sage's trusted support partner in actively managing and safeguarding the majority of the Organisation's technology infrastructure. Sage wishes to establish a collaborative and mutually beneficial partnership, rather than seeking reactive 'fix-on-fail' service provision.

Therefore, please note that this RFP's list of requirements should not be regarded as a full and complete list of the activities that Sage expects its chosen partner to perform. It should be regarded as a guide to Sage's needs but one that should be built upon by you, based on your experience and knowledge.

4.1 Service & Security Requirements

1. **Help Desk and Problem Resolution:** Provide details on:
   a. How you would provide a help desk facility and appropriately skilled technical resources to resolve issues as they arise in the technology components provided and/or supported by you;
   b. Provide details on the standard working hours for the Help Desk and the tools used;
   c. The communication channels supported;
   d. The mechanisms available for staff to monitor the status of their tickets, and
   e. The mechanisms available for Sage to monitor service performance at an Organisational level.

2. **Device Management:** Provide details on how you would perform:
   a. Proactive service monitoring of desktops, laptops, phones, and Microsoft 365.
   b. Management / patching of devices
   c. Lifecycle Management of Devices –Asset decommissioning/disposal etc. (Certificate of destruction)

3. **Licensing Advice: While the Organisation will continue to purchase and manage its licenses,** the selected IT support partner will provide expert guidance on the types and numbers of licenses that the Organisation should acquire. Provide your recommendations on how this process should work.

4. **Backups:** Provide details on how you would ensure a secure backup of our Microsoft 365 data is performed on a regular basis, how the process will be monitored and how the backups will be tested.

5. **Cyber Security:** Provide details on how you would perform key security activities, such as:
   a. Proactive monitoring & management of M365, including monitoring and improving our Microsoft Secure Score.
   b. Proactive security monitoring/ management of firewall / network / Wi-Fi security defences.
   c. Proactive security monitoring/ management of our endpoint devices.
   d. Establishment of a multi-layered security architecture that not only addresses current threats but also attempts to anticipate and mitigate future and emerging threats, focusing on both traditional and AI-driven approaches.
   e. Provision of advice in relation to the security implications/ risks relating to our use of M365/ Teams/ OneDrive/ SharePoint for external sharing, integrations etc.
   f. Delivery of staff cybersecurity awareness training through an appropriate online platform, along with regular phishing test campaigns.

6. **Reporting:** It is imperative for Sage to be provided with evidence that security and service activities are being completed in line with the IT support partner's responsibilities and best practice, including visibility

of relevant security and service KPIs to keep the Sage's Executive Team informed of current security and service health. Please provide details on:

a. How you will meet this reporting requirement – e.g. the KPIs you will monitor and report; details of the recent & planned actions included in the reports; frequency of reporting; reporting format / structure to ensure the information is appropriate to a business audience.
b. How you will engage with Sage to review security and service performance (e.g. through a regular online or in-person service meeting)

4.2 Non-Functional Requirements

1. **Business Scale and Capability:** Sage needs to be confident that its selected IT support partner is in this business for the long-term. Provide as much detail as possible about your Organisation, current ownership and management structure and its past, present and future strategy. In addition, provide information such as:
   a. How managed IT security and service provision relates to the core business of your Organisation.
   b. An overview of the management approach for the Services encompassing the key roles and an outline of responsibilities.
   c. An Organisational chart/ description detailing the structure in place to deliver the proposed service.
   d. An overview of the various teams and departments within the Organisation including specific details on headcount, locations, etc.
   e. An overview of the depth of staff, capacity and expertise within the Organisation or available within your service partners' Organisations.
   f. The criteria and process used for selecting, qualifying and contracting subcontractors and suppliers (Supplier Management).
   g. An overview of your vendor partnerships (e.g. for hardware, software, support contracts), and your ability to source, negotiate and manage contracts with vendors and suppliers.

2. **Partners and Solution Providers:** Provide details of any 3rd parties / partners who will be involved in the services proposed for Sage. For example: Will you subcontract any components of the proposed solution to third-party Organisations? If so, describe the components to be subcontracted and provide details of any agreement in place with the subcontracted firm/ individuals as well as a summary of past work that you have successfully completed together. Describe your relationships and experience with manufacturers and major distribution partners. Provide details of the hardware and solution providers that you work with and/or that you implement solutions from e.g., network security solutions that you would implement for Sage.

3. **Data Protection and Security:** Sage is regulated by the Charities Regulator and the Data Protection Commission. More importantly, we are also very aware of the very sensitive data that we handle on behalf of vulnerable people. It is important for Sage that its IT support partner can demonstrate a clear understanding of the strict data protection and IT security obligations that Sage needs to comply with. Sage requires its IT support partner to demonstrate how its internal processes align to current and emerging data protection and security standards. Provide details of how your Organisation manages its own security and how it would manage Sage's security (e.g., how Sage technology, systems and data will be secured, and how access to these data/systems from within your Organisation will be restricted, managed, reviewed). Additionally, provide evidence of how you comply with accepted industry standards and best practices for IT security and/or service management (e.g., ISO 27001, ITIL, NIST CSF). The evidence should include the scope, level, and date of any certifications or accreditations.

4. **Service Delivery Targets/ Commercial Incentives:** Sage needs to know its chosen IT support partner has clear service targets (both in terms of initial response and problem resolution) and is motivated/ incentivised to deliver a service in line with these targets. Provide details of the Security and Service Level

Agreement proposed for this engagement. For example, details of a robust and transparent service level management framework that defines, monitors and reports on key performance indicators (KPIs) – both in terms of security and service – as well as service level agreements (SLAs). Additionally, provide details of any incentives/ repercussions included in the proposed contract to ensure these services' levels are maintained.

5. **Supporting Our Staff:** Sage advocates and acts on behalf of older and vulnerable people. Our staff are dedicated and focused advocate professionals. But they may not possess advanced technical expertise. Therefore, Sage requires the chosen IT support partner's processes and staff to offer patient and understanding assistance. It is essential that all interactions are conducted with a supportive and encouraging approach to ensure our staff can effectively utilise the technology and services provided. Please provide details on your proposed approach.

6. **Working with our current IT Service Provider:** Sage's current IT service provider is an individual who has provided IT support services to Sage for many years, knows our staff well, and is highly-regarded by our team. Should a new IT support provider be selected, Sage is interested in understanding if or how a collaboration between this individual and the new provider could work. Please describe if or how you could integrate their expertise and familiarity with our Organisation into your proposed support structure. While this is not a mandatory requirement, it is a preference. We also recognise that any proposed approach is subject to further discussion and negotiation with the current provider.

7. **Draft Pro-Forma Contract and Insurance Policy:** Sage assumes that the standard client contract used by the chosen IT support partner will apply to the Sage engagement. It is important that we review the draft pro-forma contract as part of the RPF assessment so we can identify early in the process whether there are any contract clauses which may require external review. Provide Sage with your draft pro-forma client contract as well as the details of your insurance policy relating to both staff and service delivery.

8. **Policy Development/Advice:** Describe the role you could play in assisting Sage to develop and maintain appropriate policies (e.g., data privacy / protection, IT security, data retention, cybersecurity, fair use policy, business continuity planning, incident response planning).

9. **Service Governance, Ongoing Management and Strategy Consulting:** It is important to Sage that there are regular face-to-face meetings with the chosen IT support partner to review recent activities but more importantly, to consider future trends, potential issues, and opportunities. Sage recognises that the IT support provider is a critical partner to the Organisation and want the IT support partner to continuously review how practices can be improved to optimise our business strategy. Sage would value regular / scheduled in-person time with the chosen partner. Provide details of how you will engage with Sage to review security and service performance and to proactively advise Sage on security / service / technology trends.

10. **Client Satisfaction Monitoring:** Provide details on how you monitor customer satisfaction and quality assurance on an ongoing basis and how we might benefit from this process.

11. **Client References:** Provide contact details for at least two clients of a similar size / scale as Sage.

4.3 Implementation Requirements

Sage needs to be confident that should a new IT support provider be selected; the service handover and any ensuing security / service uplift will be managed appropriately to minimise operational and security risks.

Provide a high-level work plan that demonstrates the steps for integrating Sage with your service for Day 1 and beyond. This plan should consider the existing technology infrastructure at Sage and propose the necessary improvements to enhance our infrastructure and data management.

For example, The Day 1 plan should provide the following information:

1. Key activities
2. Timing
3. Information/resource requirements from Sage and/or its current IT Service Provider
4. Deliverables
5. Key milestones, checkpoints, and other decision points.
6. The type and frequency of status reporting to be provided
7. The proposed approach for ongoing engagement with Sage and proposed approach for regular reviews with Sage to assess progress vs plan
8. The inventory of technical/configuration and user documentation that will be delivered as part of the implementation, (e.g., Documents to capture the policies assigned to each device, user access controls, password policies, user procedures)

Post Go-Live, you should also provide information on if / how you can assist Sage in improving its current infrastructure (e.g. centralised device management; firewall; wired network; wireless network; switches).

4.4 Pricing and Billing Requirements

To enable Sage to assess the likely cost of engaging your services, as much transparency and detail as possible would be appreciated.

A detailed pricing grid has been provided as a separate Excel template. This pricing grid aligns to the service requirements outlined in section 4.1, as well as some suggested ‘value-add services’ that you may choose to offer. Please complete this grid.

Alternatively, if you are providing pricing in a separate format, please ensure all pricing information is provided in one place in your response. Please also ensure your format lists each of our stated requirements and the costs for each requirement.

Where appropriate, you can add extra lines to the bottom of the pricing grid (or at the bottom of your chosen pricing table) for any additional service or product offerings you wish to include in your proposal.

At a minimum, Sage needs to understand:

- What costs are fixed or variable (and what drives the variations - e.g. cost per user; cost per device; cost per license; cost per call)
- What costs are upfront/once-off or ongoing
- What costs are optional
- Any bundling / multi-year / pre-pay discounts available
- Whether each price is ex-VAT or inclusive of VAT
- Any assumptions you have made when pricing this service

5 RFP and Selection Process

It is Sage's intention to evaluate & select an IT support partner by **Monday 28th July**, with a view to the selected IT Support Provider being in place by **Friday 29th August**.

Project Name	Sage IT Support / Cyber Security Partner Selection	
Contact Point for RFP	lara.gallagher@sageadvocacy.ie,	
Target Timelines	RFP Circulated	Thursday 26th June
	Your Notification of "Intent to Respond" Deadline *(Refer to section 5.1)*	**By Friday 4th July**
	"Meet Sage"/ site survey (*optional* 45-min on-site or online meeting) *(Refer to section 5.2)*	On Monday 7th July
	Deadline for receipt of any queries *(Refer to section 5.3)*	By Friday 11th July
	RFP Response Deadline	**By Friday 18th July**
	RFP Review and Follow-up by Sage	From Monday 21st July
	Preferred Vendor Announced by Sage	**On Monday 28th July**
	Contract Finalisation	By Friday 1st August
	Implementation Completion	**By Friday 29th August**
	Post-Live Remediation / Follow-Up Completed	By Friday 19th September

5.1 Your "Intent to Respond"

If you intend to respond to the RFP, please email lara.gallagher@sageadvocacy.ie, by the "Intent to Respond" deadline, **Friday 4th July**.

In addition, please also:

- Confirm the contact details of the individual responsible for coordinating your RFP response.
- Confirm whether you wish to "Meet Sage" and/or perform a site survey on the date mentioned in the earlier table, whether your preference is to do this in-person or online, and whether there are specific times that you are / are not available on that day.

5.2 Meet Sage

If you wish to meet Sage in Ormond Quay or online, a time can be agreed for **Monday 7th July**.

This meeting is optional and for your benefit - You will not need to present or discuss your proposal on this day. It is primarily an opportunity for you to meet Sage and /or to perform a site visit / walkthrough.

5.3 RFP Queries

If you have any queries in relation to this RFP, please send your query to lara.gallagher@sageadvocacy.ie, no later than the "Queries" deadline, **Friday 11th July**.

All queries received will be responded to within 2-3 working days.

To ensure fairness and transparency, all queries (whether received via email or during any in-person / online meetings) and their respective responses will be distributed to all participants in the RFP process.

5.4 Response Submission Process, Content and Format

- Your response to this RFP will be used by Sage to ascertain your suitability as its IT support partner.

- Your proposal should respond in as much detail as possible to each question and point raised throughout this RFP, but in particular in 'The Requirements' section. You are free to include additional information if you deem it appropriate.

- If you wish to provide additional supporting material for one or more questions, label attachments clearly and reference them in your response. Please note Sage may not review all supporting material. You must ensure you provide relevant responses (and costings) within your main response document.

- Submit your response in PDF format, with pricing information in Excel format. Each response / pricing line item should include a clear reference to the requirement to which the response / item relates.

- All files associated with your response should be sent as attachments in one email to lara.gallagher@sageadvocacy.ie, and no later than **Friday 18th July**. If you wish to encrypt these files, you may send them within a single encrypted ZIP file. The password for the ZIP file should be sent via SMS to Lara Gallagher on 086 142 7897.

5.5 Review & Selection Process

RFP Review

As shown in the timelines stated in the table earlier, Sage has set a challenging timeframe to evaluate the responses received.

During this period, we do not require a formal presentation of your proposal, but we would appreciate your availability via email or phone to answer any follow-up queries we may have. We may also ask to meet with you during this review process if we need to discuss specific elements of your proposal in more detail.

Selection Criteria

Sage will evaluate each response using a number of criteria to select the most appropriate partner.

The following summarises the major qualitative areas that will be evaluated, and your response to each of our requirements and any additional information provided will feed into the evaluation.

- Financial considerations
- Proposed service
- Industry expertise and experience
- Previous relevant experience
- Current client base
- Vendor strength and stability
- Reporting capabilities and Account management
- Demonstrated customer service quality and support
- Demonstrated partnership approach
- Engagement Details (e.g., Approach to ongoing / in-person engagements)

5.6 Terms and Conditions

No Obligation:

The submission of a proposal shall not in any manner oblige Sage to enter into a contract or to be responsible for the costs incurred by your Organisation in responding to this request.

Agreement of Non-Disclosure:

This document is considered proprietary and shall not be disclosed to any other party. It is designed, developed and submitted to potential partners of Sage solely for the benefit of Sage.