netcentrix

Hospice IT & Cyber Security

A practical guide for hospice leaders, clinical teams, and operations staff.
Created by Netcentrix

Trusted by Hospices

Microsoft Solutions Partner

Why Secure IT Matters

In a hospice, technology should work quietly in the background. When it is reliable and secure, it supports care without drawing attention to itself. When it is not, even small issues can cause disruption and unnecessary worry.

Good IT and cyber security work in layers. Much like armour, each layer has a role to play. Some protect devices and systems from everyday risks. Others safeguard sensitive patient and donor information. Together, they create a strong but unobtrusive level of protection that allows hospice teams to focus on what matters most.

This playbook is designed to be practical and easy to use. It explains the common IT and cybersecurity risks hospices face, and the simple steps that can reduce disruption, improve reliability, and strengthen security. There is no technical jargon and no one-size-fits-all approach. Instead, the guidance reflects how hospices really work, with mixed systems, limited budgets, and teams made up of staff and volunteers.

Whether you are responsible for managing IT day-to-day or providing oversight and managing risk, this playbook is here to help you clearly understand where your current protections are working well, where gaps may exist, and what practical steps will make the biggest impact.

This isn't about technology for technology's sake. It's about technology that works quietly in the background — protecting time, enabling care, and preserving comfort and dignity.

In this playbook, you'll discover:

- The foundations of safe, reliable IT
- Common cyber security risks facing hospices
- Practical actions to improve protection
- Real-world case studies and simple checklists
- How Netcentrix supports hospices

The Hospice IT Landscape

Modern hospices rely on technology across many areas:

Clinical Systems

- Electronic patient records (EPR)
- Medication management systems
- Appointment scheduling and triage
- Secure internal communications

Operational Systems

- HR and volunteer management platforms
- Fundraising and donation systems
- Cloud tools such as Microsoft 365
- Telephony, WiFi, and office devices

Retail Systems

- Point-of-sale (POS) systems in charity shops
- Stock and inventory management
- Pricing, promotions, and gift aid tracking
- Secure handling of customer and donor data
- Connectivity between shops and head office systems

Common Challenges

- Multiple systems that do not always integrate smoothly
- Volunteers using personal devices
- Hardware that is ageing or inconsistent
- Remote teams or community-based care
- Need for reliable access to critical data at all times

Technology can enable hospice teams to work more efficiently, but only if it is reliable, secure and supported.

The Main IT and Cyber Risk Facing Hospices

Hospices rely on technology to support care delivery, fundraising, administration and communication.
The most common risks include:

Phishing and Social Engineering
Emails or messages that appear to come from trusted colleagues, suppliers or healthcare bodies may ask for login details or sensitive information. These attacks are increasingly convincing and rely on human error rather than technical weaknesses.

Ransomware
Cyber criminals may encrypt files and demand payment to restore access. Even a small incident can disrupt access to patient records, schedules and essential systems.

Data Loss or Misuse
Lost laptops or phones, unsecured file sharing and weak passwords can expose sensitive patient, donor or staff data.

Outdated Systems
Devices or software that are no longer updated may contain known vulnerabilities that can be exploited.

Cyber Security Essential Layers

Layer One: Devices and Access
Every device used in a hospice plays a role in day-to-day care and operations. Laptops, desktops, tablets and phones all need to be reliable and properly protected. Key actions in this layer include:

- Keeping devices up to date with security patches
- Encrypting laptops and mobile devices
- Using strong passwords and multi-factor authentication
- Managing user access when staff or volunteers join or leave

These steps reduce everyday risks and help prevent small issues from becoming larger problems.

Layer Two: Systems and Data
Hospices hold sensitive information, from patient records to donor and staff data. Protecting this information is essential for trust, continuity and compliance. This layer focuses on:

- Keeping systems and applications up to date
- Controlling who can access different types of data
- Using secure backups that are tested regularly
- Making sure data can be restored quickly if needed

Good data protection ensures information is available when needed and protected when it is not.

Layer Three: Email and Online Threats
Email remains one of the most common entry points for cyber incidents. Phishing messages are designed to look genuine and often create a sense of urgency. Practical steps include:

- Email filtering to block known threats
- Clear guidance on how to report suspicious messages
- Simple awareness training for staff and volunteers
- Reducing reliance on email links for sensitive actions

This layer helps teams recognise and stop threats before they cause disruption.

Layer Four: People and Everyday Use
Technology only works when it fits how people actually work. In hospices, teams often include staff, volunteers and remote workers with different levels of confidence using IT. This layer focuses on:

- Clear, simple IT guidance
- Regular but light-touch awareness training
- Support that is easy to access and responsive
- Processes that reduce the chance of mistakes

The aim is to support people, not burden them.

Layer Five: Monitoring, Support and Continuity
Even well-protected systems need ongoing care. Monitoring and proactive support help identify issues early and reduce the risk of unexpected downtime. This layer includes:

- Proactive monitoring of systems
- Clear escalation routes for issues
- Regular testing of backups and recovery plans
- Ongoing review of risks and improvements

Strong support helps keep systems running smoothly and care uninterrupted.

Bringing the Layers Together
Each layer on its own offers protection. Together, they create a balanced and dependable approach to IT and cyber security.

The purpose of these layers is not defence for its own sake, but to reduce disruption and protect time for care. When technology is reliable and secure, hospice teams can focus on providing comfort, dignity and support to patients and families.

A Practical Cyber Security Framework

A simple model for hospices is **Protect – Detect – Respond – Educate.** This framework helps hospices keep technology reliable and secure while giving teams confidence to focus on care.

Step	What it means	Examples / Actions
Protect	Build strong foundations	MFA, encrypted devices, secure WiFi, regular patching, controlled admin access, robust backups
Detect	Identify issues early	24/7 monitoring, automated threat alerts, regular vulnerability scans
Respond	Act quickly when something happens	Incident response plan, tested backups, clear staff communication
Educate	Reduce human error	Phishing awareness, cyber hygiene training, role-specific guidance

Hospice IT & Cyber Checklist

Layer 1: Devices and Access
☐ All laptops and tablets are kept up to date
☐ Devices are encrypted in case they are lost or stolen
☐ Multi-factor authentication is enabled where possible
☐ User access is reviewed when staff or volunteers change

Layer 2: Systems and Data
☐ Key systems are regularly updated and supported
☐ Access to sensitive data is limited to those who need it
☐ Data is backed up securely
☐ Backups are tested to ensure they can be restored

Layer 3: Email and Online Threats
☐ Email filtering is in place to reduce phishing risks
☐ Staff and volunteers know how to report suspicious emails
☐ Links and attachments are treated with caution
☐ Shared accounts are avoided where possible

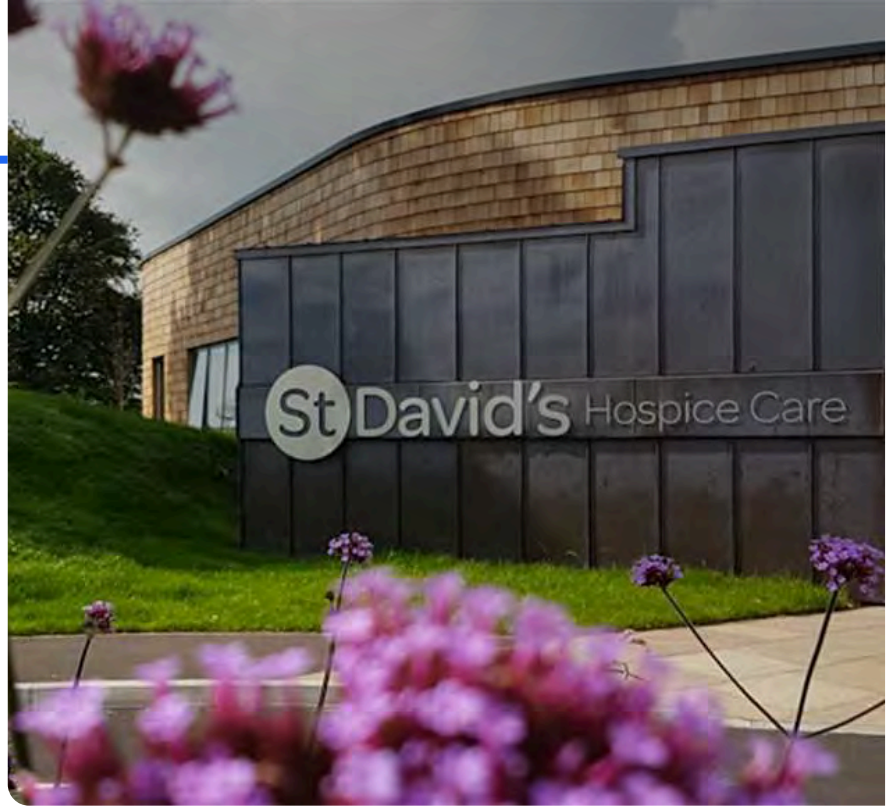
Layer 4: People and Everyday Use
☐ Staff and volunteers receive simple IT and cyber guidance
☐ Clear processes exist for common IT tasks
☐ Support is easy to contact when something goes wrong
☐ Technology is easy to use and not overly complex

Layer 5: Monitoring and Continuity
☐ Systems are monitored for issues or failures
☐ There is a clear plan for responding to IT incidents
☐ Backups and recovery processes are reviewed regularly
☐ IT risks are reviewed as systems or teams change

Next Steps
If you are unable to tick all of these boxes, you're IT isn't secure. Our free IT & Cyber Health Check can help identify practical improvements that reduce disruption and protect time for care.

Free IT & Cyber Heath Check

Your Hospice in Safe Hands



In the Spotlight: St David's Hospice

Challenge

Keep IT systems secure and reliable across five servers, so staff can work smoothly without disrupting patient care - a challenge familiar to many hospices managing multiple sites and remote teams.

Actions

- Phased Windows 11 upgrade delivered with strategic account management, ensuring correct software, strong security controls, and best practice
- Validated, documented, and handed back to Netcentrix Service Desk for ongoing oversight

Outcome

- Systems fully supported and more secure
- Improved performance and reliability for remote staff
- Staff can focus on patients, not technology

Why other hospices work with Netcentrix

We combine deep experience supporting hospices with proactive IT and cyber security, so teams can focus on care knowing their systems are safe, reliable, and fit for purpose.

> *"Netcentrix delivered this plan from inception to completion, and the project ran very effectively. As a hospice we do not employ any internal resource and Netcentrix delivered this project in a true partnership style, updating and communicating at pivotal milestones. We are really happy with the project delivery and outcome."*
>
> ***Margaret Hollings***
> *Commercial Director*

Working with Netcentrix

Other IT providers might offer standard support or generic cyber security services. We do things differently.

- We understand hospices - We understand how hospice teams, volunteers, and patients work. Our IT and cybersecurity services are designed around real hospice environments — not generic, one-size-fits-all models.
- Friendly, human support - Our service desk speaks plain English and responds promptly. No jargon, no unnecessary delays — just clear, calm, and reassuring support when it's needed most.
- Proactive, not reactive - We continuously monitor systems, keep devices up to date, and regularly check backups, helping to identify and resolve issues before they disrupt care.
- Designed around the way you work - Whether your teams are based across multiple sites, working in the community, or operating remotely, we keep your IT running smoothly, securely, and reliably.
- Affordable and transparent - Our services are designed to align with hospice budgets, offering clarity on costs without cutting corners or introducing unnecessary complexity.
- An educational approach - We don't just fix problems. We help staff and volunteers understand how to use technology safely and confidently, reducing risk and building long-term resilience.
- Care always comes first - We understand that every IT issue takes time away from patient care. By managing technology on your behalf, we help your teams focus on care, comfort, and dignity.
- Trusted by hospices and charities across the UK - Our experience supporting hospices and charities across the UK means you can be confident your systems are in safe and capable hands.

Get In Touch

Tel. 0333 035 4111
Web. netcentrix.com/contact

Matrix Industrial Park, Eaton Ave Buckshaw Village, Chorley, PR7 7NA