netcentrix

A Practical Guide To AI And Cyber Security For Hospices

Trusted by Hospices
★★★★★

HUNTRESS

Microsoft Solutions Partner

About this guide

This guide is for hospice leaders, managers and teams who want to understand what AI can do for their organisation, and how to manage the cyber security risks that come with it.

This guide is designed to help you have better conversations internally, ask the right questions, and take practical steps forward without feeling overwhelmed.

AI and cyber security might seem like separate topics, but they are not. AI is creating real opportunities for hospices to save time, reduce admin and support staff. At the same time, the same technology is making cyber attacks more sophisticated and harder to spot, and understanding both sides is important.

The The Hospice Context

Hospices face a unique set of pressures that make technology decisions more complex than in many other organisations.

Mixed resources. Many hospices have small IT teams, sometimes one or two people covering everything. There is very little capacity to absorb new technology without careful planning.

A mixed workforce. Paid staff, volunteers, clinical teams, fundraisers, retail workers and administrators all work under the same roof, often with very different levels of digital confidence.

Sensitive data across multiple areas. Patient and clinical records, donor and supporter information, retail transactions, finance, payroll, HR and volunteer records all sit across different systems. Protecting that data matters enormously, and so does using it well.

Public trust. Hospices are deeply embedded in their communities. A data breach, a poorly handled AI incident or a scam that goes wrong does not just have financial consequences. It can damage the relationships that hospices depend on.

Funding pressure. Every technology decision needs to be justified. If a tool does not save time, reduce risk or improve care, it is hard to defend the cost.

Part 1: AI and Productivity

What AI actually means for hospices

There is a lot of noise around AI at the moment. Much of it is either overly technical or full of hype. The reality for most hospices is more straightforward.

AI tools that are already available within Microsoft 365 can help with everyday tasks. They do not require a large budget or a technical team to get started. They work best when they are solving a real problem, not when they are adopted because everyone else seems to be doing it.

The most useful question to ask before looking at any AI tool is this - what problem are we actually trying to solve, and how much time or effort would solving it save?

If the answer is 30 seconds a week, the case is weak. If the answer is several hours of manual admin per day, or a task that is causing stress or burnout for staff, the case becomes much stronger.

Where AI can genuinely help

These are the areas where hospices are already finding real value from AI tools:

Day to day administration

- Summarising long email threads so staff can catch up without reading everything
- Rewriting complicated or technical emails into plain English
- Drafting responses to common enquiries
- Taking meeting notes and turning them into a summary or action list

Fundraising and supporter engagement

- Processing Gift Aid forms, including splitting scanned documents automatically
- Finding and filing documents without manual naming and sorting
- Supporting bid writing and grant applications
- Identifying duplicate supporter records and improving data quality
- Searching image banks to find suitable photos for campaigns and communications

HR, training and onboarding

- Creating training materials and session plans more quickly
- Drafting job descriptions with consistent language
- Supporting new starter onboarding with guided information
- Reviewing and updating policies and documents

Governance and compliance

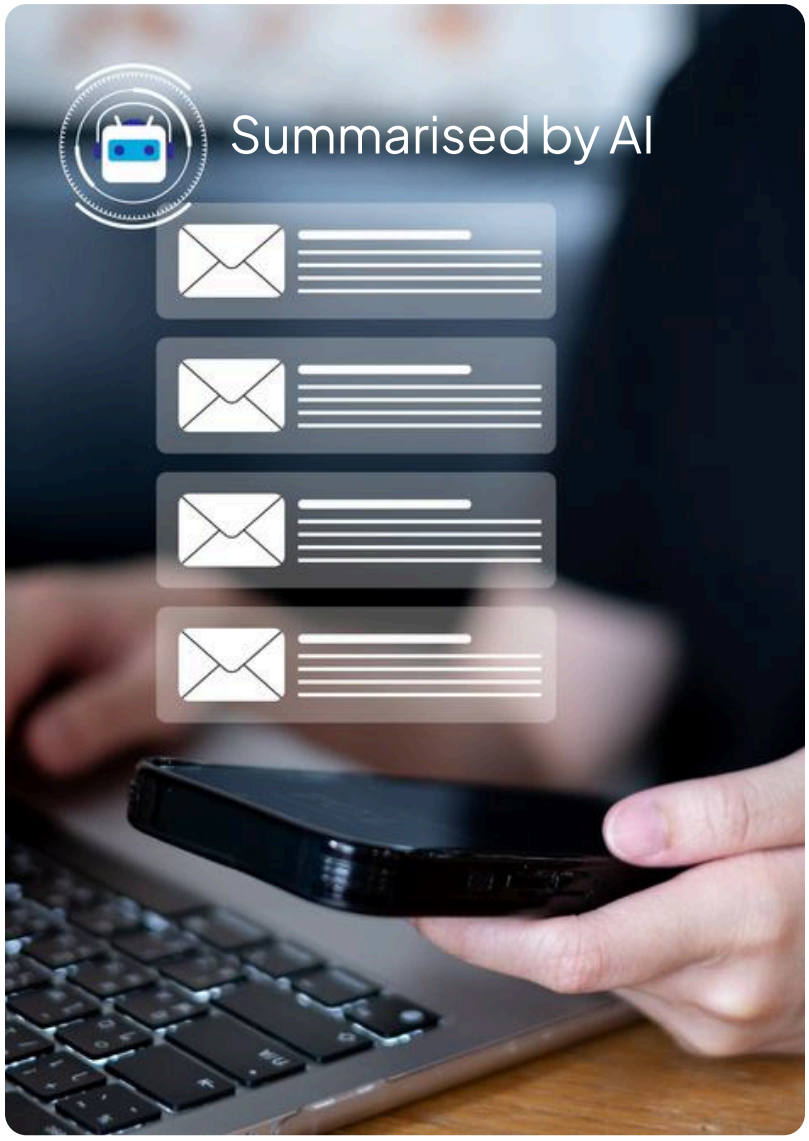
- Supporting DPIA drafts and information governance documents
- Summarising lengthy regulatory guidance into plain English
- Helping prepare board reports and briefing papers

Accessibility and inclusion

- Translating communications for patients, families or volunteers who speak other languages
- Making documents easier to read for people with visual or reading needs

Clinical and operational teams

- Transcribing end of shift notes to reduce documentation time
- Summarising handover information
- Helping staff find information quickly from internal documents and policies



Starting Small and Building Confidence

One of the most common mistakes organisations make with AI is trying to do too much too soon. A better approach is to start with one or two practical use cases where the benefit is clear, build confidence among a small group of willing staff, and grow from there.

It also helps to be honest about digital confidence across your organisation. If some staff are still getting to grips with the basics of Microsoft 365, jumping straight to AI tools will create more anxiety than value. The foundation needs to be solid before you build on top of it.

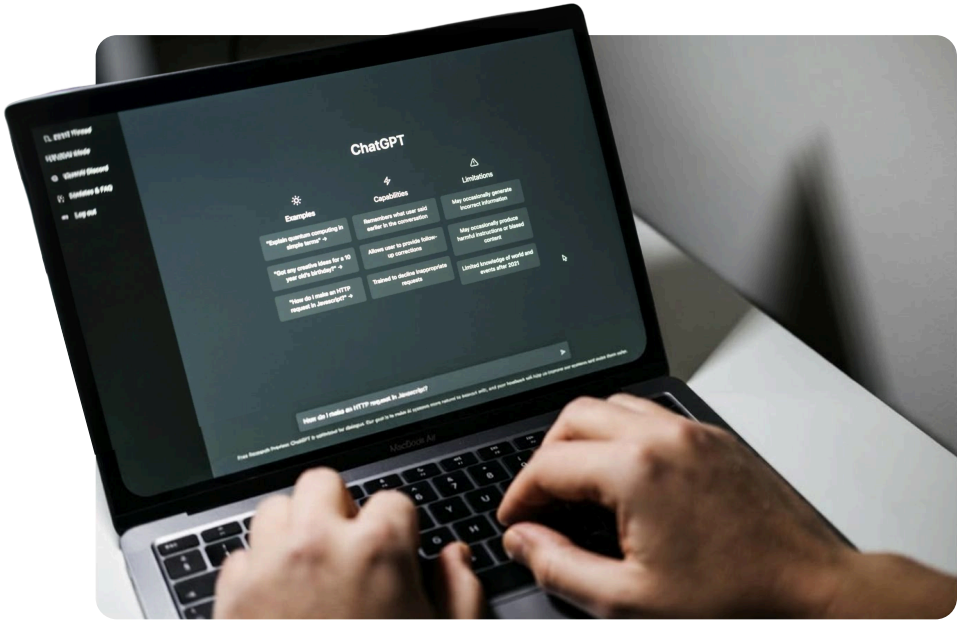
Practical starting points tend to work better than generic AI training. Showing a fundraising team how to use AI to summarise a long email thread, or showing a clinical administrator how to draft a handover note more quickly, lands better than a theoretical session about what AI is and how it works.

The Question of Governance and Policy

If your organisation does not have an AI usage policy, it is worth creating one. This does not need to be a lengthy document. It needs to answer a few important questions clearly.

- What AI tools are approved for use within the organisation?
- What information can and cannot be entered into AI tools?
- Who is responsible for reviewing AI outputs before they are used?
- How should staff raise concerns or questions about AI?

The reason this matters is that many staff are already using AI tools in their personal lives and may be using them at work without realising the risks. Free public tools like ChatGPT are not designed for organisational use.



Information entered into them may be used to train future models and is not protected in the same way as information that stays within a governed Microsoft 365 environment.

An AI policy does not need to ban anything. It needs to set clear expectations so that staff feel confident about what they can and cannot do.

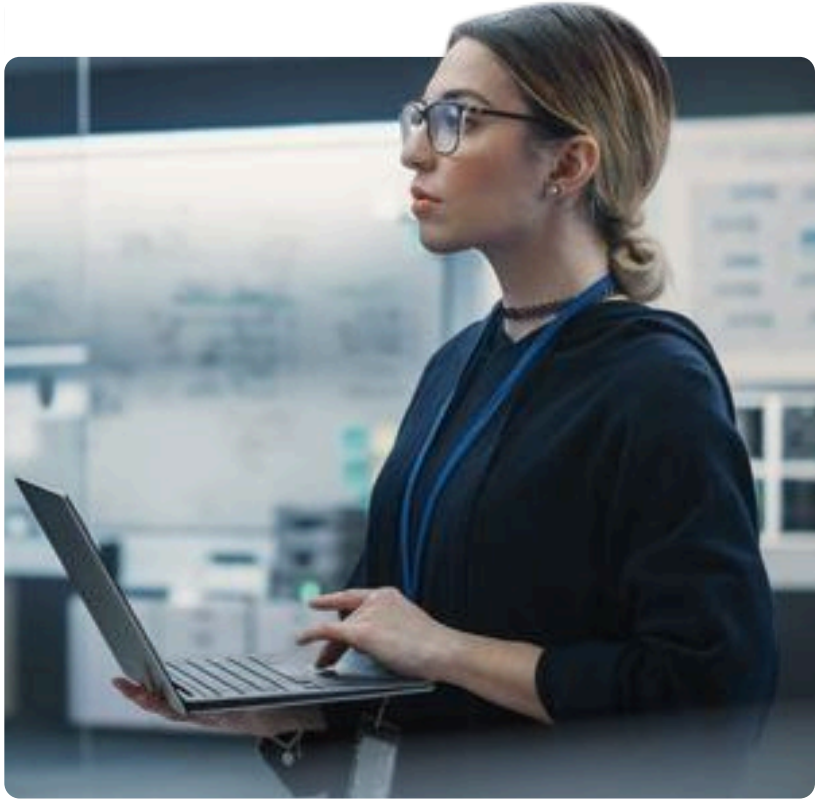
Data and Why It Matters Before AI

AI tools work best when the information they draw from is accurate, well organised and up to date. For many hospices, this is a challenge.

Supporter data, donor records, volunteer information and operational data often sit across multiple systems with limited connection between them. The same person might appear as a donor in one system, a café customer in another and a former patient family member in a third, with different spellings of their name in each.

Before expecting AI to deliver significant value, it is worth identifying where your most important data sits and how reliable it is. Some practical starting points:

- Identifying and merging duplicate supporter or donor records
- Agreeing on naming conventions and file structures across the organisation
- Understanding which systems hold which information and how they connect



These steps might not feel exciting, but they are what make AI tools genuinely useful rather than just impressive in a demonstration.

Microsoft 365 and Copilot Readiness

If your organisation uses Microsoft 365, you already have access to a growing set of AI tools. Microsoft Copilot is the most widely discussed, but it is not the right starting point for every organisation.

Before considering Copilot licences, it is worth asking a few honest questions.

- Is Microsoft 365 being used consistently across the whole organisation?
- Is SharePoint set up in a way that makes information easy to find?
- Do staff know where to store and find documents?
- Is there any governance around how Teams and SharePoint are used?

If the answer to most of these is no, adding Copilot will surface disorganised information and create confusion. The right first step is getting the foundations right.

For organisations that are not yet ready for full Copilot licences, Microsoft Copilot agents offer a more contained starting point. Agents can be built around specific tasks and draw only from approved information sources. Examples include a policy agent that helps staff find answers from internal documents, a new starter agent that handles common onboarding questions, or a job description agent that creates consistent adverts from approved templates.

Training and Learning Resources Worth Knowing About

Makers Making Change
A Neil Squire Program

Microsoft Change Makers is a free, non-technical credential from Microsoft focused on real nonprofit use cases. It is suitable for non-IT staff and leaders who want to build confidence with Microsoft tools and AI.

Microsoft Elevate

Microsoft Elevate offers broader learning resources for organisations moving toward AI adoption.

365 TRIBE
ADOPTION. CHAMPIONED

365 Tribe is a hospice-specific Copilot training programme with structured cohort-based learning. It is designed around hospice workflows and requires Copilot licences to participate.

A practical workshop or promptathon, where hospice teams work through shared use cases together, is often more valuable than sitting through a generic presentation about AI. If you are interested in this kind of session, it is worth exploring with your technology partner.

Part 2: Cyber Security

Why cyber risk is increasing for hospices

Cyber attacks on charities and healthcare organisations are increasing. Hospices are not immune, and being small does not make you a less attractive target. Attackers look for organisations with valuable data and limited security controls, and hospices often fit that description.

The most important shift in recent years is that attacks are increasingly focused on identity rather than just devices. In the past, the main concern was someone getting malware onto a computer. Now, the bigger risk is often an attacker gaining access to a staff member's email account or Microsoft 365 login. From there, they can read emails, access files, impersonate the account holder, set up forwarding rules and move through the organisation without being detected.

AI is making this worse. Phishing emails that used to be easy to spot because of poor spelling or odd phrasing are now well written, personalised and convincing. Attackers can use AI to research their targets, craft believable messages and automate parts of an attack that previously required significant effort.

The response to this cannot be training alone. Awareness matters, but people make mistakes. The organisations that recover well from cyber incidents are the ones that had the right controls in place before anything went wrong.

The Most Important Controls To Have In Place

Multi-factor authentication

If your organisation does not have multi-factor authentication switched on for all accounts, this is the single most important thing to address. MFA means that even if an attacker obtains a password, they cannot access the account without a second form of verification. It is one of the most effective controls available and it does not require significant investment to implement.

Conditional access

Conditional access allows you to set rules around how and where Microsoft 365 accounts can be accessed. For example, you can restrict access to approved devices, flag logins from unusual locations, or block access from countries where your organisation has no legitimate activity. These controls significantly reduce the risk of a compromised account being used without detection.

Endpoint protection

Basic antivirus is no longer sufficient. Endpoint detection and response tools, commonly known as EDR, go further by monitoring for suspicious behaviour on devices rather than just blocking known threats. They provide much greater visibility into what is happening across your organisation and support faster response when something goes wrong.

Microsoft 365 configuration

Many organisations are running Microsoft 365 with settings that have never been reviewed. Default settings are not always the most secure. Areas worth checking include external sharing permissions in SharePoint and OneDrive, guest access in Teams, email authentication records, and whether admin accounts have appropriate protections in place. A Microsoft 365 security review can identify gaps in configuration that may not be obvious from day to day use.

Phishing awareness and reporting

Training staff to recognise phishing emails is important. But the bigger gap in many organisations is not recognition, it is reporting. If ten members of staff spot a suspicious email and delete it without telling anyone, the eleventh person may still click on it. There is no alert, no investigation and no way to stop the next attempt. Make it easy for staff to report suspicious emails. Make clear that reporting is always the right thing to do, even if it turns out to be a false alarm. Track reporting rates, not just click rates from phishing simulations.

Backups and recovery

Even with strong controls in place, one mistake can still trigger a serious incident. Ransomware attacks can encrypt or destroy data across an entire organisation within hours. Backups are the safety net. Good backups are run daily, stored separately from the main environment, held in immutable storage so they cannot be deleted or encrypted by an attacker, and tested regularly. A backup that has never been restored is an assumption, not a guarantee.

Incident response planning

If something goes wrong, the cost of not knowing what to do next can be significant. Having a basic incident response plan in place, even a short document that covers who to contact, what to isolate and what not to do, can make a real difference to how quickly and effectively an organisation recovers.

Cyber insurance

Cyber insurance is worth reviewing carefully. Many organisations have a policy but have not checked whether it actually covers their most likely scenarios, or whether the security controls the policy requires are actually in place. A policy that does not pay out when you need it is not protection.

Cyber Essentials

Cyber Essentials is a government-backed certification that covers five core security controls. It provides a useful baseline and can support insurance applications, tendering processes and integrations with partner organisations.

Cyber Essentials (CE) is worth pursuing, but it should be understood as a starting point of your cyber journey, rather than a complete answer. Cyber Essentials covers the basics, but many of the threats facing hospices today require controls that go further.

What Trustees and Boards Need to Understand

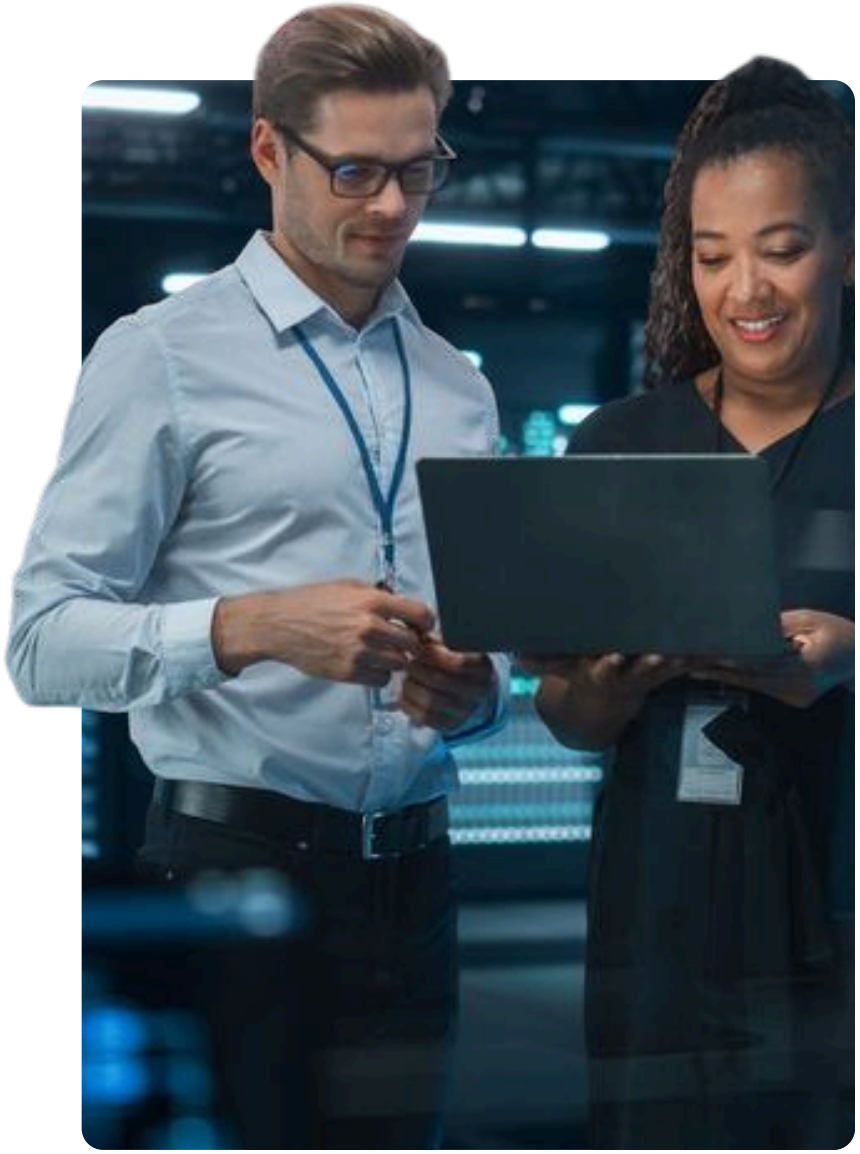
Cyber security and AI are not just operational issues. They are governance issues, and boards need to be engaged with both.

Trustees do not need to be technical experts. But they do need to understand the risks the organisation is carrying, what is being done to manage those risks, and what the consequences of a serious incident could look like.

Some useful questions for boards to ask:

- Do we have an AI usage policy, and do staff know about it?
- Are we confident that sensitive data is not being entered into public AI tools?
- When did we last review our Microsoft 365 security configuration?
- Do we have multi-factor authentication in place for all accounts?
- Have our backups been tested recently?
- Does our cyber insurance policy cover our most likely risk scenarios?
- Do we have a plan for what to do if we experience a cyber incident?

If these questions cannot be answered confidently, that is important for the board to have.



Where to Start

If this guide has raised questions about where your organisation currently stands, a good first step is an honest assessment of your current position across both AI readiness and cyber security.

For AI, the key questions are whether your Microsoft 365 environment is well organised, whether you have an AI usage policy, and whether there are one or two specific use cases where AI could genuinely save time or reduce admin.

For cyber security, the key questions are whether MFA is switched on for all accounts, whether your Microsoft 365 configuration has been reviewed, whether your backups are tested and stored separately, and whether staff know how to report suspicious activity.

You do not need to tackle everything at once. Identify the most significant gaps and address them one at a time, with support from a technology partner who understands the pressures hospices are under.

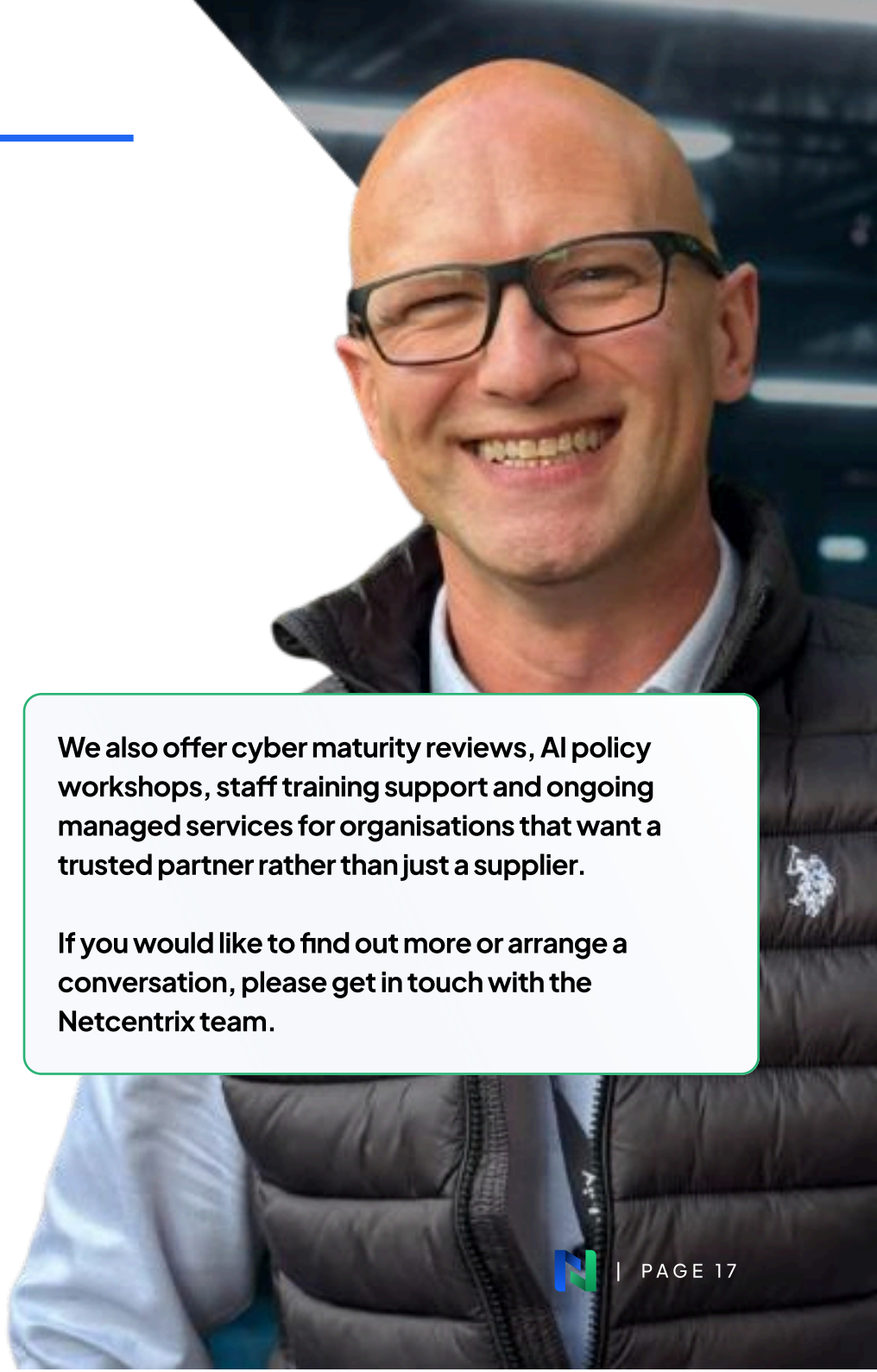
How Netcentrix Can Help

Netcentrix works with hospices and charities across the UK, supporting them with Microsoft 365, cyber security, AI readiness and technology strategy.

We offer a free Microsoft 365 tenancy audit for hospice organisations. This gives you an objective view of your current security configuration and Copilot readiness, with clear recommendations for next steps. It requires appropriate admin access, is carried out under NDA, and access is removed once the review is complete.

We also offer cyber maturity reviews, AI policy workshops, staff training support and ongoing managed services for organisations that want a trusted partner rather than just a supplier.

If you would like to find out more or arrange a conversation, please get in touch with the Netcentrix team.



We also offer cyber maturity reviews, AI policy workshops, staff training support and ongoing managed services for organisations that want a trusted partner rather than just a supplier.

If you would like to find out more or arrange a conversation, please get in touch with the Netcentrix team.

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

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