

CASE STUDY

Strengthening Jisc Audit Readiness with a Single Cyber Security Dashboard for **Carmel College**

Carmel College is a single-site sixth-form college supporting approximately 2,500 students and 250 staff across eight distinct buildings. A dedicated, four-person IT team manages around 1,500 Windows-based assets and is responsible for maintaining secure, resilient infrastructure that keeps systems reliable to support uninterrupted teaching and learning, as well as meeting regulatory and audit obligations. The college was looking for a solution that could address the Jisc audit requirements while also strengthening day-to-day security operations.



Type of Organisation

Catholic Sixth-Form College.

Situation

Following a Jisc cyber security assessment, Carmel College needed a unified, auditable asset register, automated asset discovery and clearer vulnerability visibility to strengthen compliance and cyber resilience.

Solution/Results

By implementing the ITHealth Dashboard, the college replaced multiple legacy tools with a single platform, gaining full visibility of all assets, automating vulnerability management, significantly improving patch compliance, and strengthening Jisc and internal audit readiness.



“

The Jisc audit highlighted areas for improvement around asset management, vulnerability visibility and log management. We had multiple systems that didn't talk to each other, which made evidencing compliance complicated.”

KEVIN BURKE
Head of IT Services, Carmel College

The Situation

Like many further education providers, Carmel College is required to undergo regular cyber security assessments as part of its funding obligations. A recent Jisc audit set out a series of recommendations, including the implementation of a college-wide asset management register and automated asset discovery. The college also recognised the need to strengthen vulnerability management and improve overall visibility across the IT estate to simplify compliance.

At the time, the IT team relied on several standalone tools for logging, vulnerability scanning, and asset management. Each system operated independently, requiring manual cross-referencing to answer audit queries. Logging was limited: records were only retained for 30 days, which made it difficult to investigate incidents or provide historical evidence for audits. Producing evidence was time-consuming and complex, and visibility across the estate was fragmented.

For a four-person IT team supporting a large student and staff population, this approach was unsustainable. The college needed an integrated, proactive way to manage cyber risk that would simplify audit preparation while strengthening day-to-day security operations.

“

Having used ITHealth for six years at my previous NHS Trust, I knew it would work here too. Now we have a complete view of every asset and its patch status, with vulnerabilities flagged automatically. Managing the IT estate is simpler and more proactive - we can spot and fix issues as they arise.”

PHIL MUSCART
Infrastructure Engineer, Carmel College

The Solution

Carmel College implemented the ITHealth Dashboard to create a single, unified view of its IT estate. With automated network discovery and a comprehensive asset register in place, the college immediately addressed one of the key Jisc audit requirements.

Asset management, vulnerability tracking, patch monitoring, and device activity oversight were consolidated into a single platform, replacing multiple legacy tools. While ITHealth does not provide full event logging, it does retain historical information on user logins, device status, and patching, giving the team longer-term visibility to track activity and respond efficiently to audit queries. Instead of manually checking separate systems, the team can now identify high-risk vulnerabilities directly from the ITHealth Dashboard and remediate them quickly - often with simple patch updates.

The Infrastructure Engineer's experience with ITHealth at a previous NHS Trust also enabled a smooth and rapid deployment.

“

When senior leadership say they're going to audit us, it's no longer daunting. We're confident everything we need is in the ITHealth Dashboard and we can just pull the necessary details and reports.”

KEVIN BURKE, Head of IT Services, Carmel College

The impact was immediate. Within just five weeks, the number of devices unpatched for over 90 days fell from 900 to 61 — and this continues to improve. Daily reporting, which previously required manual effort, is now generated instantly, allowing the team to prioritise work efficiently. The ITHealth Dashboard has become the team's primary operational tool, used every day to monitor patch compliance, identify risks, and maintain the college's security posture.

Results and Next Steps

Since implementing the ITHealth Dashboard, Carmel College has moved from “reactive firefighting” to “proactive fire prevention” in managing cyber risks. Vulnerabilities are surfaced automatically, enabling the team to prioritise and remediate high-risk issues before they escalate - reducing the need for manual threat hunting.

The college has achieved Cyber Essentials and is preparing for Cyber Essentials Plus, with audit confidence significantly strengthened. Recommendations from the Jisc assessment have been systematically addressed, with several findings moving from amber to green following ITHealth implementation.

Beyond compliance, the ITHealth Dashboard also supports strategic planning. The team can identify ageing devices, low disk space, and upgrade requirements without physically inspecting rooms -saving valuable time and enabling data-driven investment decisions.

For further education providers facing growing cyber security expectations, Jisc scrutiny, and limited IT resources, Carmel College's experience demonstrates how a unified, audit-ready dashboard can simplify compliance, strengthen security, and support uninterrupted teaching and learning.

As Kevin Burke, Head of IT Services at Carmel College notes:

*“It feels as though there's a lot of goodwill from ITHealth - if we suggest a development or improvement, they look into it rather than dismiss it. **It's the kind of partnership that makes a real difference.**”*

Ready to increase your security visibility of your estate?

Call: 0115 987 6339

Email: info@ithealth.co.uk

Visit: www.ithealth.co.uk

About ITHealth

ITHealth provides trusted cyber security and access management solutions to the UK public sector. With over 30 years' experience and a strong NHS pedigree, we help organisations protect critical services, sensitive data, and complex IT estates. Our ITHealth Dashboard delivers unified asset intelligence, improving visibility, reducing risk, supporting compliance, and enhancing operational efficiency.

Registered Office: ITHealth, 10 Churchill Park, Private Road, No 2, Colwick, Nottingham, NG4 2HF