

Supplier assurance after the PHP alert

The NCSC warned on 21 October 2026 that every version of PHP was affected by a critical flaw. This briefing sets out what it advised and how the DfE cyber security standard turns that advice into routine.

For trust leaders, IT and business leads · 25 October 2026

What happened

The NCSC reported that PHP had released a security update for a critical issue that may allow attackers to execute commands on any web server running PHP, under certain conditions without authentication. It said organisations using any version of PHP are affected.¹

Its advice: identify PHP systems across the estate, prioritising internet-facing ones; update to the latest version, internet-facing first, then internal; apply temporary mitigations or take a system offline where updating is not yet possible; look for signs of compromise; and monitor vendors for updates to products and services that bundle PHP.¹

What trust leaders are discussing

The most replied-to Data and Digital thread of the week, posted the day after the alert, collected confirmations from suppliers of school websites, governance platforms, data integration and pension services, and asked who had heard from whom.

What the DfE standard asks for

The cyber security standard for schools and colleges asks for:²

- vulnerability fixes rated critical or high risk applied within 14 days of release, and DfE security instructions within 5 working days;
- licence expiry dates in the contracts register and end-of-support dates in the asset register, with the contracts register reviewed every term;
- outsourced IT providers able to explain how they meet the standards;
- supplier assessments when new cloud contracts are procured.

It also sets out who to tell when an incident happens, from IT support and the SLT digital lead through to governors or trustees, the DfE sector cyber team and, for a high-risk data breach, the ICO within 72 hours.²

Where technology helps

A register that answers the question

Add two columns to the contracts register: whether the supplier hosts a web-facing service for the trust, and the contact for security notices. When the next alert lands, filter the register and send one message to every relevant supplier the same day. Record each reply in the same place, and the board report writes itself.

Questions for the leadership team

1. Can the trust list every web-facing supplier within the hour?
2. Who sends security queries to suppliers, and where are the replies kept?
3. When did the board last see a cyber risk update?

Evidence base

1. NCSC, Critical security issue affecting PHP (21 October 2026)
<https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php>
2. DfE, Cyber security standards for schools and colleges (updated 16 September 2026)
<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges>

Prepared by TransforMATive from public sources and anonymised, aggregated themes from sector discussion.
thetransformative.com