

Statement for data protection officers: PHP security vulnerability, October 2026

22 October 2026 · Realsmart

Summary

On 21 October 2026 a critical security vulnerability was announced in PHP, the software that WordPress and millions of other websites run on. Realsmart installed the official fix on every website and system we host for schools the same day.

We then reviewed our systems for any sign that the vulnerability had been used against us. We found no evidence that any school's website, systems or personal data was affected, and we have not identified a personal data breach. Schools do not need to take any action.

The vulnerability

The PHP project published fixes for two related flaws, CVE-2026-109618 and CVE-2026-109619, sometimes referred to as "php2shell". In some circumstances they could allow an attacker on the internet to run their own code on a web server without logging in. The PHP project rated them critical.

The flaws affected almost every organisation that runs PHP, not Realsmart in particular. News of the flaws first appeared on 20 October; the official fixes and full details were released on the afternoon of 21 October.

What we did and when

All times are on 21 October 2026, UK time.

Time	Action
Morning	Identified every Realsmart system that runs PHP and which versions each uses, before the fix was released.
14:37	The PHP project released the fixed versions.
By 15:05	Switched off, on every system, the PHP feature one of the flaws could be reached through, as an extra layer of protection.
By 19:00	Installed the fixed versions of PHP on every Realsmart-hosted website and system, and confirmed each one was running them.
By 19:15	Removed PHP entirely from systems that did not need it, and updated the template our new servers start from, so every new server starts with the fixed version.

Our websites stayed available throughout. Any brief interruption while each server restarted on the new version lasted seconds.

Our investigation and findings

We found no evidence that the vulnerability was used against any Realsmart system.

On 21 October we reviewed every server we run for schools, covering the period from 20 October, when news of the flaws first appeared:

- server and application error logs, for the crashes and memory errors an attack would cause
- our load balancer's records of website traffic
- programs running on each server, and any network connections they had made
- recently created or changed files in temporary and upload folders, where an attacker would leave tools
- scheduled tasks, user accounts and access keys, where an attacker would try to keep access

We saw the routine automated scanning that every website on the internet receives, including attempts to use older, unrelated PHP flaws. All of it was rejected, and none of it was linked to any error, unexpected change or unknown program.

As with any investigation of this kind, we cannot prove a negative: our logs do not record the full contents of every web request. Our conclusion rests on the absence of any of the signs a successful attack leaves behind.

Personal data and reporting

We have not identified a personal data breach, so on the evidence available there is nothing for your school to report.

Under UK GDPR your school is the data controller and Realsmart is your data processor. If we become aware of a personal data breach affecting your school's data, we will tell you without undue delay, as Article 33(2) requires of us. Whether to notify the Information Commissioner's Office remains your school's decision, and we will give your data protection officer any information they need to make it.

What your school needs to do

Nothing. Your website, logins and content are unchanged, and there is nothing to update or reset. If your website runs on Smartpress, staff who sign in to it will also see a short notice about this on their dashboard until 4 November.

For questions about this statement, contact support@realsmart.co.uk.

Sam Gray

CTO, Realsmart