Suffolk County Council

Schools' IT Newsletter

JANUARY 2026

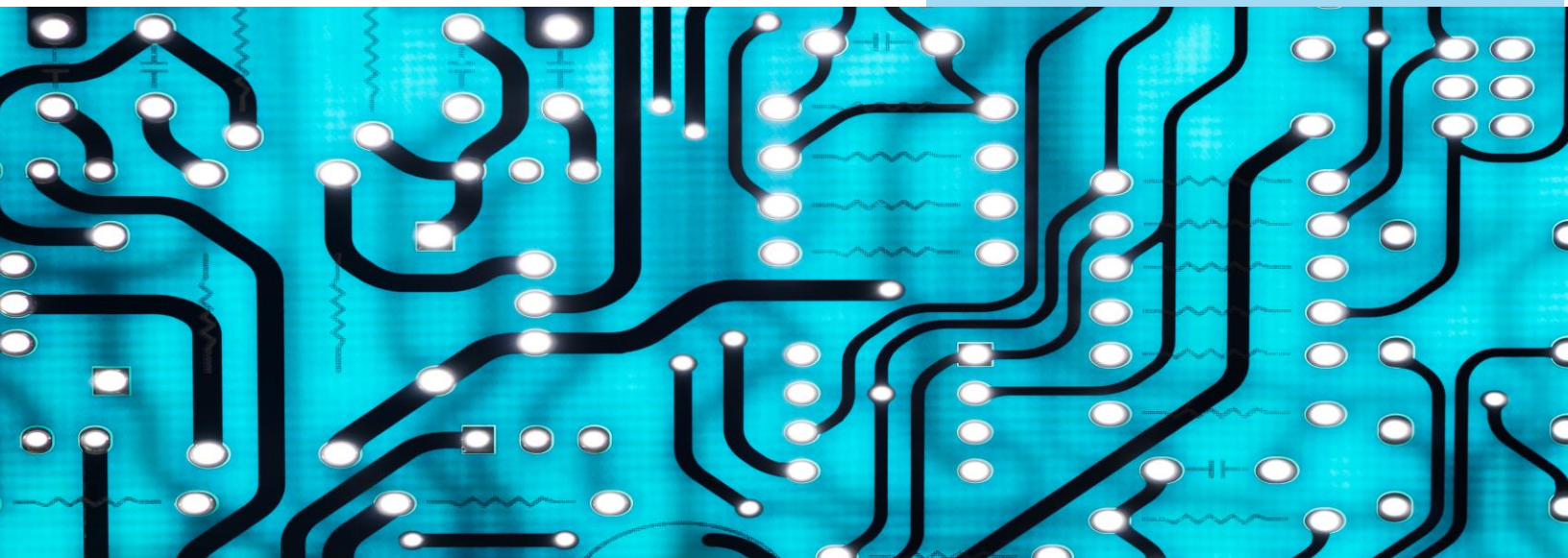
Included in this month's issue:

The Schools' IT Team would like to welcome all our colleagues back after what we hope was a pleasant and peaceful Christmas.

We wish you all a very happy new year and look forward to continuing to offer support with your IT Services for 2026.

A Brief reminder re: FortiPortal Access

To help keep access secure, please notify the IT Service Desk whenever your school changes IT support or when staff with FortiPortal access leave. This allows us to promptly deactivate old accounts and set up new ones without delay. Details of how to contact the Service Desk are at the end of this newsletter.



SPRING CENSUS TRAINING 2026

Census training for 2025/26 will be available as pre-recorded content and published in the Arbor Resource Library.

Below you will find the dates of when this content will be available to view:

- Spring Census Dry Run - Monday 5 Jan, 1pm
- CES Census - Thursday 15 Jan, 1pm
- Spring Census Day - Thursday 15 Jan, 1pm

This will not be a live webinar and so there will not be any ability to ask questions on the census.

If you require assistance on the dry run, then please do not hesitate to log a call and we will get back to you.

The census line will be available from Wednesday the 14th of January until Tuesday 20th of January, 0830hrs to 1600rs each day the line is open.

SPRING CENSUS 2026

FAO HEADTEACHER, ADMIN OR STAFF DEALING WITH THE CENSUS

The Spring Census is approaching, and the school must identify an activity at a period in the school day for all classes. This is dictated by the last digit in the school establishment number. If you cannot remember what the school establishment number is then this can be seen from "school details".

During the Spring Census, schools are asked to record a specific classroom activity at a set time.

- The time slot is determined by the last digit of the school's establishment number.
- If staff do not recall the establishment number, it can be found in the "School Details" section of your MIS (Management Information System).

School > School Details > School Details

The timings can be obtained from the DfE guidance.

However, below, you can identify the period of activity the DfE is interested in:

0, 1 or 5 The selected time is one hour before the end of morning School

2, 3 or 6 The selected time is one hour after the start of afternoon school

4, 7, 8 or 9 The selected time is one hour after the start of morning school

The spring census in Arbor will become available on the return after the Christmas break, as detailed in the article above.

In the previous spring census, schools have asked as to whether the period can be changed. This can be changed where the selected time is not appropriate to the school timetable:

- Assembly
- Trips
- Sickness

Guidance on unusual circumstances.

This will also report on school class sizes, there is legislation that covers school infant class sizes.

Where the class sizes exceed the limits to these class sizes then a code needs to be used to explain the reason, DfE have guidance on the codes that should be used.

Arbor will have a webinar for the spring census closer to the time when the dry run becomes available, like the Autumn Census.

Other guidance from the DfE as to the data items in the census.

Guidance from the DfE on checking data.

The DfE have a YouTube link to explain the collect site.

Arbor Guidance on the census can be available from here.

Please do test you login credentials prior to needing them to upload your census as it can take the DfE a while to reset passwords.

DfE Login.

The notes that were used in the Autumn Census will be the same notes that will be used in the Spring Census and the Summer Census.

The spring census date that the schools should have in your diaries is the 15th January 2026. The DfE closing date for this census is the 11th February 2026, however, to add schools in getting authorised the LA require schools to upload and submit their census by the 23rd January 2026.

SCHOOL CYBER SECURITY UPDATE

Date – 16/12/2025

Please provide this document to your member of staff responsible for IT

Links to patching the vulnerabilities:

- CVE-2025-55182 - Remote Code Execution Vulnerability in React and Next.js Frameworks: December 2025
- APSB25-105 : Security update available for Adobe ColdFusion - https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd44
- APSB25-115 : Security update available for Adobe Experience Manager - https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd46
- APSB25-118 : Security update available for Adobe DNG SDK - https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd48
- APSB25-120 : Security update available for Adobe Creative Cloud Desktop - https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd4c

Vulnerabilities

Remote Code Execution Vulnerability in React and Next.js Frameworks: December 2025

CVE-2025-55182

SIR – Critical

CVSS score – 10.0

URL - Remote Code Execution Vulnerability in React and Next.js Frameworks: December 2025

Adobe Security Bulletin:

APSB25-105 : Security update available for Adobe ColdFusion
APSB25-115 : Security update available for Adobe Experience Manager
APSB25-118 : Security update available for Adobe DNG SDK
APSB25-119 : Security update available for Adobe Acrobat Reader
APSB25-120 : Security update available for Adobe Creative Cloud Desktop

~~~~~~
~~~~~~

APSB25-105 : Security update available for Adobe ColdFusion
Originally posted: December 9, 2025

Summary: Adobe has released security updates for ColdFusion versions 2025, 2023 and 2021. These updates resolves critical and important vulnerability that could lead to arbitrary file system write, arbitrary file system read, arbitrary code execution, security feature bypass, and privilege escalation.
Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Learn more: https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd44

Priority Rating:

Adobe categorizes these updates as priority 1.

https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd45

~~~~~~

APSB25-115 : Security update available for Adobe Experience Manager

Originally posted: December 9, 2025

Summary: Adobe has released updates for Adobe Experience Manager (AEM). These updates resolve vulnerabilities rated critical and important. Successful exploitation of these vulnerabilities could result in arbitrary code execution or privilege escalation. Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Learn more: https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd46

Priority Rating:

Adobe categorizes these updates as priority 3.

https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd47

~~~~~~

APSB25-118 : Security update available for Adobe DNG SDK

Originally posted: December 9, 2025

Summary: Adobe has released an update for the Adobe DNG Software Development Kit (SDK) for Windows and macOS. This update resolves critical and important vulnerabilities that could lead to arbitrary code execution and memory exposure, or application denial-of-service. Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Learn more: https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd48
Priority Rating:

Adobe categorizes these updates as priority 3.

https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd49

~~~~~~

APSB25-119 : Security update available for Adobe Acrobat Reader

Originally posted: December 9, 2025

Summary: Adobe has released a security update for Adobe Acrobat and Reader for Windows and macOS. This update addresses critical and moderate vulnerabilities. Successful exploitation could lead to arbitrary code execution and security feature bypass. Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Learn more: https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd4a

Priority Rating:

Adobe categorizes these updates as priority 3.

https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd4b

~~~~~~

APSB25-120 : Security update available for Adobe Creative Cloud Desktop

Originally posted: December 9, 2025

Summary: Adobe has released an update for the Creative Cloud Desktop for macOS. This update includes a fix for an important vulnerability that could lead to application denial-of-service in the context of the current user. Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Learn more: https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd4c

Priority Rating:

Adobe categorizes these updates as priority 3.

https://t-info.mail.adobe.com/r/?id=t44bcfe14,836750e1,c0e4cd4d

Threats landscape

Microsoft Silently Patches Windows LNK Flaw After Years of Active Exploitation

Microsoft has silently plugged a security flaw that has been exploited by several threat actors since 2017 as part of the company's November 2025 Patch Tuesday updates, according to ACROS Security's 0patch.
The vulnerability in question is CVE-2025-9491 (CVSS score: 7.8/7.0), which has been described as a Windows Shortcut (LNK) file UI misinterpretation vulnerability that could lead to remote code execution.
"The specific flaw exists within the handling of .LNK files," according to a description in the NIST National Vulnerability Database (NVD). "Crafted data in an .LNK file can cause hazardous content in the file to be invisible to a user who inspects the file via the Windows-provided user interface. An attacker can leverage this vulnerability to execute code in the context of the current user."
In other words, these shortcut files are crafted such that viewing their properties in Windows conceals the malicious commands executed by them out of the user's sight by using various "whitespace" characters. To trigger their execution, attackers could disguise the files as harmless documents.

Google Adds Layered Defenses to Chrome to Block Indirect Prompt Injection Threats

Google on Monday announced a set of new security features in Chrome, following the company's addition of agentic artificial intelligence (AI) capabilities to the web browser.

To that end, the tech giant said it has implemented layered defenses to make it harder for bad actors to exploit indirect prompt injections that arise as a result of exposure to untrusted web content and inflict harm.

Chief among the features is a User Alignment Critic, which uses a second model to independently evaluate the agent's actions in a manner that's isolated from malicious prompts. This approach complements Google's existing techniques, like spotlighting, which instruct the model to stick to user and system instructions rather than abiding by what's embedded in a web page.

"The User Alignment Critic runs after the planning is complete to double-check each proposed action," Google said. "Its primary focus is task alignment: determining whether the proposed action serves the user's stated goal. If the action is misaligned, the Alignment Critic will veto it."
The component is designed to view only metadata about the proposed action and is prevented from accessing any untrustworthy web content, thereby ensuring that it is not poisoned through malicious prompts that may be included in a website. With the User Alignment Critic, the idea is to provide safeguards against any malicious attempts to exfiltrate data or hijack the intended goals to carry out the attacker's bidding.

Security Tip of the month

Be aware of seasonal scams.

SCHOOLS' MAIL SERVICE - MFA/SSPR

Just a further reminder that effective of 3rd December 2025 MFA registration became mandatory, upon activation of the MFA policy users are now prompted to complete MFA registration at the login screen. A deferral period of up to 14 days will be available; however, once this period has elapsed, users will be required to register immediately, and the deferral option will no longer be accessible.

These measures have been put in place to enhance security by ensuring that even if one authentication factor is compromised, unauthorized access is significantly reduced.

Please also note that request forms for new mailboxes, deletions and resets have been updated on our website. Please do not save these forms to your own devices for future use, as they are constantly being updated and should an incorrect/out of date form be submitted this will be rejected by the IT Service Desk resulting in delays with your requests.

You can find further details of the schools' mail service on our website IT services for schools and academies - Suffolk County Council

CONTACTING THE IT SERVICE DESK!

Please note that the Schools IT Services mailbox is for sales enquiries and is only monitored periodically. Therefore, if you have a query with regards to a new service, please send an email to schoolsitservices@suffolk.gov.uk.

All standard incidents and service requests ***must*** be raised via the IT Service Desk on 01473 265555 or via itservicedesk@suffolk.gov.uk otherwise this will result in any responses being delayed.

Our offices are open from 8.30am to 5pm Monday - Friday