Suffolk County Council

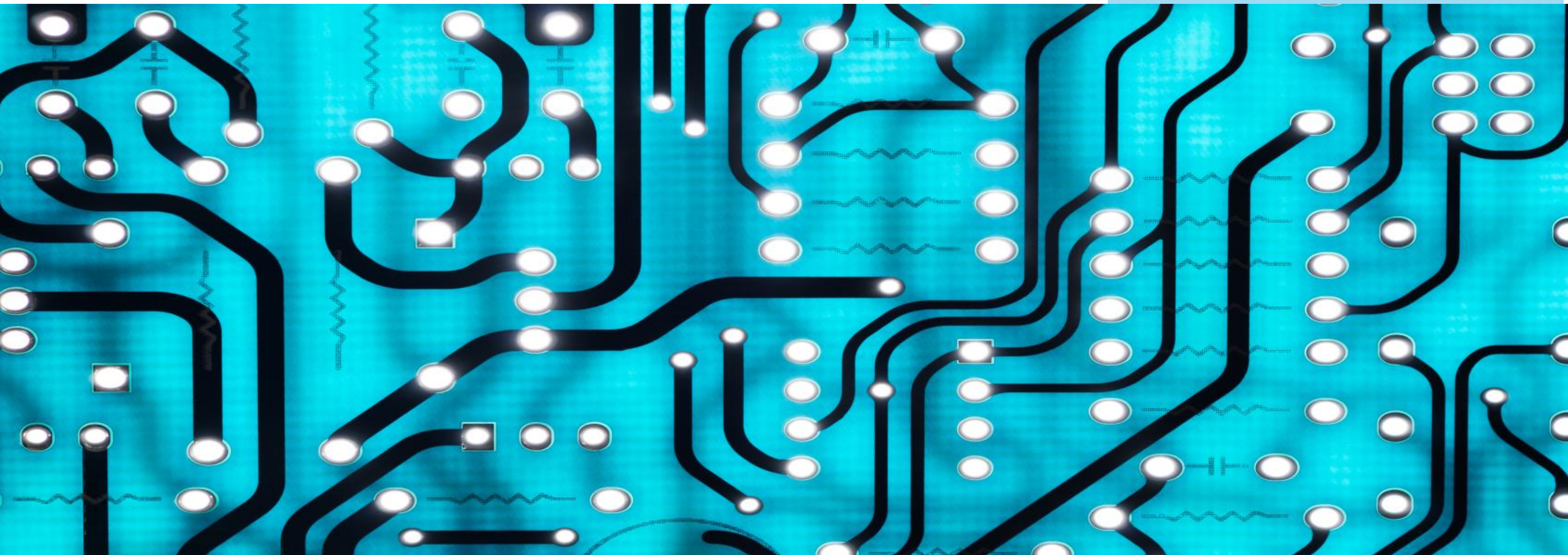
Schools' IT Newsletter

JUNE 2025

Included in this month's issue:

Schools O365 Mail Service

SCC are continuing to receive requests for new emails from generic/shared mailboxes. Please see the article below where you will find instructions on how to request new mailboxes or delete mailboxes for staff that no longer work in the school.



JUNE – ARBOR WEBINARS
FAO HEADTEACHERS/ADMIN

The upcoming Arbor webinars for June are as follows:-

Auto Absence Showcase

Thursday 5th June, 11am-12 noon.

https://arbor-hq.circle.so/c/webinars/auto-absence-showcase

Arbor Comms Showcase

Tuesday 10th June, 11am-12 noon.

https://arbor-hq.circle.so/c/webinars/arbor-comms-showcase

New School Year Setup

Steps 1-5 (for both Primary and Secondary schools)

Tuesday 10th June, 2pm-3pm.

https://arbor-hq.circle.so/c/webinars/new-school-year-setup-steps-1-5-463be0

Steps 6-9 (for Primaries only)

Monday 23rd June, 11am-12 noon.

https://arbor-hq.circle.so/c/webinars/new-school-year-setup-for-primaries-steps-6-9

Steps 6-9 (for Secondaries only)

Monday 23rd June, 2pm-3pm.

https://arbor-hq.circle.so/c/webinars/new-school-year-setup-for-secondaries-steps-6-9-aa8c42

Arbor Perform showcase

Thursday 12th June, 11am-12 noon.

https://arbor-hq.circle.so/c/webinars/arbor-perform-showcase

You do not have to attend or watch all these webinars unless the are relevant to your school. But we do recommend schools register for the New school year setup webinars, if you are unable to watch these live, you will be sent a link within 24 hours to watch on-demand.

END OF YEAR PROCESSES – ARBOR MIS

FAO SCHOOL BUSINESS MANAGERS/ADMIN ASSISTANTS/HEADTEACHERS

It is highly recommended to complete the end-of-year process before the school finishes for the summer break. If this process is not completed **before** the first day of term for the 25/26 academic year, it can open the school up to a lot of problems.

Arbor are hosting webinars to take you through this process on 10th and 23rd June (see info in the above article).

Additional guidance can be found on the links below:

- https://support.arbor-education.com/hc/en-us/articles/360019450358-New-School-Year-Setup-Preparation-Checklist
- https://support.arbor-education.com/hc/en-us/articles/360007860858-New-School-Year-Setup-help-and-guidance
- https://support.arbor-education.com/hc/en-us/articles/360019827838-How-and-when-do-we-do-the-end-of-year-process

SCHOOL CYBER SECURITY UPDATE

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

Links to patching the vulnerabilities:

- APSB25-29 : Security update available for Adobe Lightroom - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236e4
- APSB25-35 : Security update available for Adobe Dreamweaver - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236e6
- APSB25-36 : Security update available for Adobe Connect - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236e8
- APSB25-37 : Security update available for Adobe InDesign - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236ea
- APSB25-38 : Security update available for Adobe Substance 3D Painter - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236ec
- APSB25-40 : Security update available for Adobe Photoshop - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236ee
- APSB25-42 : Security update available for Adobe Animate - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236f3
- APSB25-43 : Security update available for Adobe Illustrator - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236f5
- APSB25-44 : Security update available for Adobe Bridge - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236f7
- APSB25-45 : Security update available for Adobe Dimension - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236f9
- APSB25-46 : Security update available for Adobe Substance 3D Stager - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236fb
- APSB25-51 : Security update available for Adobe Substance 3D Modeler - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236fd
- APSB25-52 : Security update available for Adobe ColdFusion - https://t-info.mail.adobe.com/r/?id=t3b0b8c08,ff7d8766,c07236ff

Vulnerabilities

Adobe Security Bulletin:

APSB25-29 : Security update available for Adobe Lightroom
APSB25-35 : Security update available for Adobe Dreamweaver
APSB25-36 : Security update available for Adobe Connect
APSB25-37 : Security update available for Adobe InDesign
APSB25-38 : Security update available for Adobe Substance 3D Painter
APSB25-40 : Security update available for Adobe Photoshop
APSB25-42 : Security update available for Adobe Animate
APSB25-43 : Security update available for Adobe Illustrator
APSB25-44 : Security update available for Adobe Bridge
APSB25-45 : Security update available for Adobe Dimension
APSB25-46 : Security update available for Adobe Substance 3D Stager
APSB25-51 : Security update available for Adobe Substance 3D Modeler
APSB25-52 : Security update available for Adobe ColdFusion

Threats landscape

Microsoft Fixes 78 Flaws, 5 Zero-Days Exploited; CVSS 10 Bug Impacts Azure DevOps Server

Microsoft on Tuesday shipped fixes to address a total of 78 security flaws across its software lineup, including a set of five zero-days that have come under active exploitation in the wild.

Of the 78 flaws resolved by the tech giant, 11 are rated Critical, 66 are rated Important, and one is rated Low in severity. Twenty-eight of these vulnerabilities lead to remote code execution, 21 of them are privilege escalation bugs, and 16 others are classified as information disclosure flaws.

The updates are in addition to eight more security defects patched by the company in its Chromium-based Edge browser since the release of last month's Patch Tuesday update.

The five vulnerabilities that have come under active exploitation in the wild are listed below -

- CVE-2025-30397 (CVSS score: 7.5) - Scripting Engine Memory Corruption Vulnerability
- CVE-2025-30400 (CVSS score: 7.8) - Microsoft Desktop Window Manager (DWM) Core Library Elevation of Privilege Vulnerability
- CVE-2025-32701 (CVSS score: 7.8) - Windows Common Log File System (CLFS) Driver Elevation of Privilege Vulnerability
- CVE-2025-32706 (CVSS score: 7.8) - Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2025-32709 (CVSS score: 7.8) - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

While the first three flaws have been credited to Microsoft's own threat intelligence team, Benoit Sevens of Google Threat Intelligence Group and the CrowdStrike Advanced Research Team have been acknowledged for the discovery of CVE-2025-32706. An anonymous researcher has been credited with reporting CVE-2025-32709.

Microsoft Sets Passkeys Default for New Accounts; 15 Billion Users Gain Passwordless Support

A year after Microsoft announced passkeys support for consumer accounts, the tech giant has announced a big change that pushes individuals signing up for new accounts to use the phishing-resistant authentication method by default.

"Brand new Microsoft accounts will now be 'passwordless by default,'" Microsoft's Joy Chik and Vasu Jakkal said. "New users will have several passwordless options for signing into their account and they'll never need to enroll a password. Existing users can visit their account settings to delete their password."

The Windows maker said it has also simplified the sign-in and sign-up user experience by prioritizing passwordless methods. Furthermore, the sign-in process now automatically detects the best available method on a user's account and sets that as the default.

For example, if an account has the option to sign in via a password and a "one time code," the user will be prompted to login via one time code instead of the password. Once signed in, they will then be instructed to set up a passkey for optimal protection.

The latest move by Microsoft, along with its peers Apple, Google, Amazon, and others in recent years, represents a steady march toward a passwordless future. With password-based cyber-attacks continuing to be a lucrative initial access vector for bad actors, the adoption of passkeys heralds an important step for account security.

Security Tip of the month - Be aware of social engineering - Definition - Social engineering is the practice of malicious actors attempting to gain unauthorised access to systems, information, data or an otherwise unobtainable asset through interpersonal communication techniques. This could be through manipulation, intimidation, persuasion, pity, a feeling of distress and pressure, a sense of urgency and importance, or exploiting someone's lack of understanding in something.

OFFICE 365 MAIL SERVICE FOR SCHOOLS & ACADEMIES

A reminder that O365 mailboxes **must** be requested for new starters via our website using the following link ***IT services for schools and academies | Suffolk County Council*****.** This is so that all security checks can be carried out and to ensure that there is no delay in setting up new mailboxes. All sections must be completed and ensure that the school's 3-digit code is included, the payroll number (if applicable) and the date of birth for the new user. All sections must be completed and ensure that the school's 3-digit code is included, the payroll number (if applicable) and the date of birth for the new user.

This form may be used for all members of staff including governors (*payroll number and date of birth is not required for governors*). You do not need to use a separate form for each user and it **must** be sent to the ITServicedesk@suffolk.gov.uk in order for your request to be actioned. Once the form has been received it can take up to 3 working days for the request to be processed. ***Please note that if the request is sent to any other mailbox this will result in delays with any action being taken.***

N.B. All requests must be sent from either the Headteacher or the Business Manager/Bursar (or equivalent) at the school/academy). New mailboxes cannot be requested by the new user.

Similarly, password resets for those users without payroll numbers must also be requested by means of the online form completed by the person/s listed above.

We would also like to emphasise the importance of letting us know about any members of staff that will be leaving their post in order that we can delete their mailbox in a timely manner and to ensure that the school is not charged for these mailboxes at renewal time. Please note that any requests for deletions must come from the person managing the email service within the school/academy. Again these request forms are available on our website and can be accessed using the following link ***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