

Schools' IT Newsletter

DECEMBER 2025

Included in this month's issue:



- December webinars in Arbor HQ
- Arbor -Adding a Seasonal Meal
- How to Whitelist emails/domains
- Arbor Autumn NPS (Net Promoter Survey)
- Schools' Mail Service – MFA/SSPR
- Smoothwall Decommissioning
- Schools' Broadband Service
- Cyber Security Update
- Contact Details



SCC's IT Department would like to wish all our colleagues a very Merry Christmas.

We would also like to thank you for your continued custom and we hope that you enjoy a very Happy New Year.

Please note that our IT Service Desk will be closed on 25th, 26th December and 1st January.





DECEMBER WEBINARS IN ARBOR HQ

Upcoming webinars that we feel would be beneficial for Suffolk LA maintained schools. Please visit [Arbor HQ](#) to see all webinars being held in December 2025.

Office Hours: Attendance for Primaries

Tuesday 9th December 11:00-12:00

Join us for an ask us anything, Office Hours session on the Attendance module, specially for Primaries. Bring your questions for Rosie from Customer Education and Sarah from Customer Success, and find out how you can make the most of the attendance module.

Book [here](#)

Office Hours: Attendance for Secondaries

Tuesday 9th December 14:00-15:00

Join us for an ask us anything, Office Hours session on the Attendance module, specially for Secondaries.

Bring your questions for Lauren from Customer Education and Julie from Customer Success, and find out how you can make the most of the attendance module.

Book [here](#)


Adding a seasonal meal (e.g. Christmas lunch)

If your school is providing a Christmas meal, which will be different to the normal cost of your school meals. Please view the following article on how to set this up with the Arbor MIS.

[Adding a seasonal meal \(e.g. Christmas lunch\) – Arbor Help Centre](#)

This was also covered in the Managing seasonal payments in Arbor webinar. You can rewatch this section only from minute 30:25 to 41:50.

If you require any help or support with this, please feel free to contact the ITServiceDesk@suffolk.gov.uk or call 01473 265555 to log a call for the Schools IT Team.





HOW TO WHITELIST EMAILS IN THE TOP 3 EMAIL PROVIDERS

It appears that some parents/guardians are experiencing issues with Arbor and email/domain addresses being blocked or sent to **Spam** or **Junk** folders. On occasions there is a need to 'Whitelist' email/domain addresses and we have added some instructions below for you to pass on to the parents/guardians: -

Parents need to whitelist ***.arbor.sc**, and also your school email address.


GMAIL

- Log in to your Gmail account.
- Click the gear icon (Settings) in the top-right corner and select 'See all settings'.
- Navigate to the 'Filters and Blocked Addresses' tab.
- Click 'Create a new filter'.
- In the 'From' field, enter the email address or domain you want to whitelist.
- Click 'Create filter'.
- Check the box for 'Never send it to Spam'.
- Click 'Create filter' again to save your settings.
- Alternatively, add the sender to your Contacts by opening the email and clicking 'Add to Contacts'.

OUTLOOK

- Open Outlook and go to Settings (gear icon).
- Select 'Mail' > 'Junk Email'.
- Under 'Safe senders and domains', click '+ Add'.
- Enter the email address or domain you want to whitelist.
- Click 'Save' to confirm.
- In the desktop app, go to Home > Junk > Junk Email Options.
- Navigate to the 'Safe Senders' tab and add the email or domain.
- Click 'Apply' and then 'OK'.

YAHOO MAIL

- Log in to Yahoo Mail and click the Settings icon (gear).
 - Select 'More Settings' > 'Filters'.
 - Click 'Add new filters'.
 - Name the filter and in the 'From' field, enter the email address or domain.
 - Choose 'Inbox' as the folder to move these emails to.
 - Click 'Save' to create the filter.
 - Alternatively, mark emails as 'Not Spam' if they appear in the Spam folder.
 - Add the sender to your Yahoo Contacts for extra assurance.
- 



ARBOR AUTUMN NPS (Net Promoter Score) SURVEY

FAO Teachers, School SLT, School Admin

Arbor will be sending out the Autumn 25 NPS survey from 8th to 19th December.

- Teachers will get an email on 8th then a reminder on 15th.
- School SLT/School Admin will see an in-app message. It will appear 3 times only.

Please can we encourage any users who receive an invitation, or in-app message to respond. This helps Arbor to understand usage amongst Suffolk schools and any areas our schools require further support and guidance from the team.



SCHOOLS BROADBAND SERVICE

For schools currently using our broadband service and maybe considering a change to a different provider, we kindly ask that you contact SCC first to discuss your requirements.

Services are continually evolving, and with our suppliers upgrading circuits, there may already be a new service available in your area that could provide you with an enhanced connection.

By speaking with us first, we can liaise directly with our suppliers to explore the best possible options for your school.

You will find our contact details at the end of this newsletter.





SCHOOLS' MAIL SERVICE -MFA/SSPR

We would like to remind those schools/academies that buy into the email service, if you have not already done so, to register for the new Multi-factor Authentication/Self-service password reset.

Effective of 3rd December 2025 MFA registration will be mandatory, upon activation of the MFA policy users will be 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.

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



SMOOTHWALL DECOMMISSIONING

As part of our decommissioning process, we have identified substantial traffic still passing through the legacy Smoothwall appliance on both the admin and curriculum IP ranges. Please note that this service is no longer supported and will soon be fully shut down by Smoothwall.

This traffic is likely originating from services or devices with manually configured proxy settings. To avoid disruption, please ensure these devices are updated to communicate with the new FortiGate service. Devices that are not reconfigured will lose internet connectivity once the Smoothwall appliance is retired.

Chrome – Settings > System > Open your computers proxy setting > Manual Proxy setup

Firefox – Settings > Scroll down to the bottom of the page > Network settings > Use system proxy

Edge - Settings > System and performance > System > Open proxy settings

Old Proxy settings - internet.gfl.suffolk.org.uk to be removed






SCHOOL CYBER SECURITY UPDATE

Date – 18/11/2025

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

Links to patching the vulnerabilities:

- Cisco Unified Contact Centre Express Remote Code Execution Vulnerabilities - SIR: Critical - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ>
 - Cisco Identity Services Engine RADIUS Suppression Denial of Service Vulnerability - SIR: High - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsuppress-dos-8YF3JThh>
 - Multiple Cisco Contact Centre Products Vulnerabilities - SIR: Medium - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-mult-vuln-gK4TFXSn>
 - Cisco Identity Services Engine Reflected Cross-Site Scripting and Information Disclosure Vulnerabilities - SIR: Medium - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH>
 - Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability - SIR: Critical - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-webvpn-z5xP8EUB>
 - Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability - SIR: Medium - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-webvpn-YROOTUW>
 - APSB25-106 : Security update available for Adobe InDesign - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d46>
 - APSB25-107 : Security update available for Adobe InCopy - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d48>
 - APSB25-108 : Security update available for Adobe Photoshop - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4a>
- 



- APSB25-109 : Security update available for Adobe Illustrator - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4c>
- APSB25-111 : Security update available for Adobe Illustrator Mobile - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4e>
- APSB25-112 : Security update available for Adobe Pass - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d50>
- APSB25-113 : Security update available for Adobe Substance 3D Stager - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d52>
- APSB25-114 : Security update available for Adobe Format Plugins - <https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d54>

Vulnerabilities

1) Cisco Unified Contact Center Express Remote Code Execution Vulnerabilities

CVE-2025-20354, CVE-2025-20358

SIR: Critical

CVSS Score v(3.1): 9.8

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ> ["<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ>"]

2) Cisco Identity Services Engine RADIUS Suppression Denial of Service Vulnerability

CVE-2025-20343

SIR: High

CVSS Score v(3.1): 8.6

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsuppress-dos-8YF3JThh> ["<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsuppress-dos-8YF3JThh>"]

3) Multiple Cisco Contact Center Products Vulnerabilities

CVE-2025-20374, CVE-2025-20375, CVE-2025-20376, CVE-2025-20377





SIR: Medium

CVSS Score v(3.1): 6.5

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-mult-vuln-gK4TFXSn> ["<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-mult-vuln-gK4TFXSn>"]

4) Cisco Identity Services Engine Reflected Cross-Site Scripting and Information Disclosure Vulnerabilities

CVE-2025-20289, CVE-2025-20303, CVE-2025-20304, CVE-2025-20305

SIR: Medium

CVSS Score v(3.1): 5.4

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH> ["<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH>"]

1) Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

CVE-2025-20333

SIR: Critical

CVSS Score v(3.1): 9.9

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB> ["<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB>"]

2) Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability

CVE-2025-20362

SIR: Medium





CVSS Score v(3.1): 6.5

URL: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW> ["https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW"]

APSB25-106 : Security update available for Adobe InDesign

Originally posted: November 11, 2025

Summary: Adobe has released a security update for Adobe InDesign. This update addresses critical vulnerabilities that could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d46>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d47>

~~~~~

APSB25-107 : Security update available for Adobe InCopy

Originally posted: November 11, 2025

Summary: Adobe has released a security update for Adobe InCopy. This update addresses critical vulnerabilities that could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d48>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d49>

APSB25-108 : Security update available for Adobe Photoshop





Originally posted: November 11, 2025

Summary: Adobe has released an update for Photoshop for Windows and macOS. This update resolves a critical vulnerability. Successful exploitation could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d4a>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4b>

~~~~~

APSB25-109 : Security update available for Adobe Illustrator

Originally posted: November 11, 2025

Summary: Adobe has released an update for Adobe Illustrator. This update resolves critical vulnerabilities that could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d4c>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4d>

~~~~~

APSB25-111 : Security update available for Adobe Illustrator Mobile

Originally posted: November 11, 2025

Summary: Adobe has released an update for Adobe Illustrator on iPad. This update resolves critical vulnerabilities that could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d4e>





Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d4f>

~~~~~

APSB25-112 : Security update available for Adobe Pass

Originally posted: November 11, 2025

Summary: Adobe has released a security update for Adobe Pass. This update resolves an important vulnerability that could lead to 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=t7e1726e6,82d89802,c0d96d50>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d51>

~~~~~

APSB25-113 : Security update available for Adobe Substance 3D Stager

Originally posted: November 11, 2025

Summary: Adobe has released an update for Adobe Substance 3D Stager. This update addresses critical and important vulnerabilities in Adobe Substance 3D Stager that could lead to arbitrary code execution. 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=t7e1726e6,82d89802,c0d96d52>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d53>

~~~~~





APSB25-114 : Security update available for Adobe Format Plugins

Originally posted: November 11, 2025

Summary: Adobe has released an update for Adobe Format Plugins. This update addresses critical and important vulnerabilities that could lead to arbitrary code execution and memory exposure. 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=t7e1726e6,82d89802,c0d96d54>

Priority Rating:

Adobe categorizes these updates as priority 3.

<https://t-info.mail.adobe.com/r/?id=t7e1726e6,82d89802,c0d96d55>

~~~~~

### Threats landscape

#### Microsoft Detects "SesameOp" Backdoor Using OpenAI's API as a Stealth Command Channel

Microsoft has disclosed details of a novel backdoor dubbed SesameOp that uses OpenAI Assistants Application Programming Interface (API) for command-and-control (C2) communications.

"Instead of relying on more traditional methods, the threat actor behind this backdoor abuses OpenAI as a C2 channel as a way to stealthily communicate and orchestrate malicious activities within the compromised environment," the Detection and Response Team (DART) at Microsoft Incident Response said in a technical report published Monday.

"To do this, a component of the backdoor uses the OpenAI Assistants API as a storage or relay mechanism to fetch commands, which the malware then runs."

The tech giant said it discovered the implant in July 2025 as part of a sophisticated security incident in which unknown threat actors had managed to maintain persistence within the target environment for several months. It did not name the impacted victim.

### Security Tip of the month

Attend cybersecurity awareness training/keep up to date with the ever-changing cyber landscape





## CONTACT 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](mailto: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](mailto:itservicedesk@suffolk.gov.uk) otherwise this will result in any responses being delayed.

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

