Schools' IT Newsletter

JULY 2025

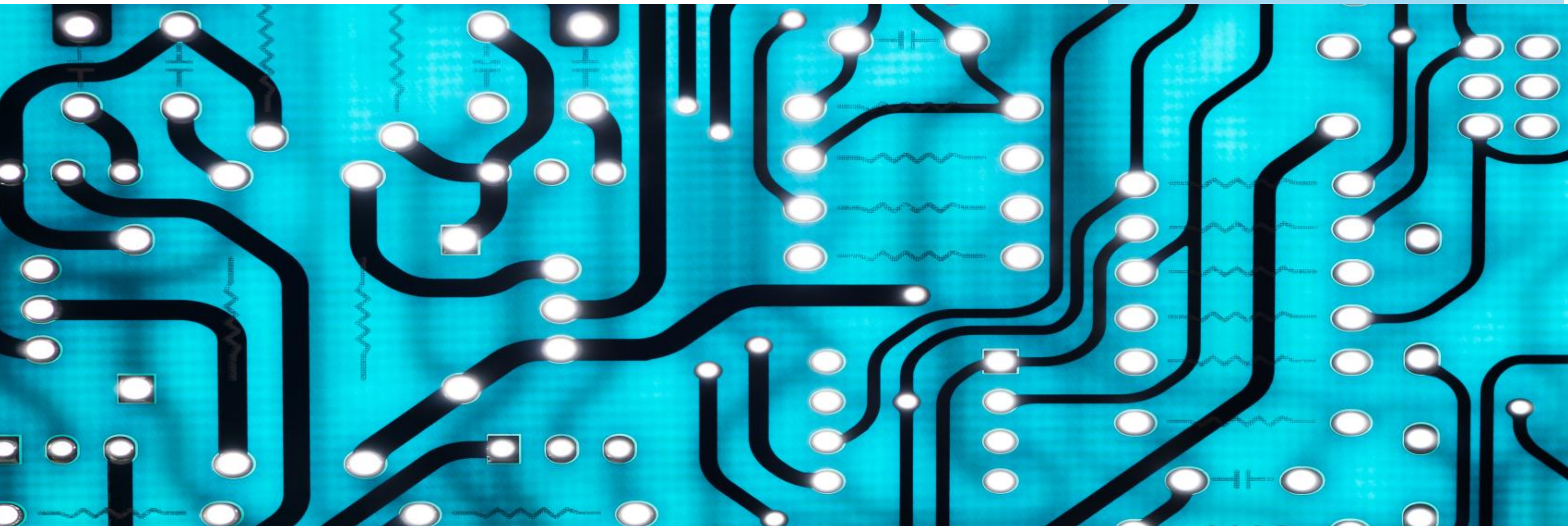
Included in this month's issue:

<u>Notification of Changes to schools' email service:</u>

Just a reminder that we will be making changes to the schools' email service with the introduction of Multi Factor Authentication (MFA).

Keep a look out for emails from Suffolk IT MFA, that will include details of the next steps that you will need to take.

Please also see the article below for some further information



USEFUL ABILITY - TO ALLOW APPLICANTS PARENT/GUARDIANS ACCESS TO PARENT APP

Several schools have now indicated that they would like their future applicants to access the parent portal for consent requests etc.

Parent portal access for applicants needs to be enabled; this does not exist by default. This can be undertaken by using the following guidance:

- Navigate to Students > Parents & Guardians > Parent Portal Settings.
- Ensure that “Applicant Parents Login” is enabled.

If you would like to see what the parent/guardian sees on login to the parent app, you would require permission to do this. The following guidance will enable a member of admin staff this permission.

- Open the staff profile of the staff member that requires the permission.
- On the left, expand the area for “Roles and Permissions”.
- Select Permissions.
- Once the permissions have loaded, select the “Student Profile” tab.
- In the search box that says “Search this table” type in “log in” without the speech marks.
- There should be an option for “Guardians: Log in as guardian”, you would have to enable this.
- This now enables the user to view Arbor as the parent would see it and test what you want them to access or do.

To view a parent’s access, you need to navigate to a parent/guardian profile, and you should see a button on the right-hand side in a grey box which says “Login in to Parent Portal as guardian”.

This does log you out of Arbor as a user however, you can now see what the parent/guardian can see in the parent app. To return as your own login, log out as the parent/guardian and log back in using your own details.

This ability is useful when navigating parent issues with what they can see or not see.

SCHOOLS' PARENT PORTAL

As schools are starting to use Parent Portal to arrange parent meetings, payments for clubs, meal and trips, some parents that have children at different schools have experienced issues with accessing the Parent Portal APP.

This is due to the control of access being at the school level, i.e. the school can reset the password, set the level of access, set prices for items/events, etc.

Additionally, if a parent has more than one child there have been several times that a parent has paid into the wrong child's account. Due to the level of access being set at the school level, a parent can experience a different level of access between portals.

The easiest solution to this would be to use a different email address for each portal access.

However, a parent can use the same email address if they choose the correct school in the dropdown on the login page. Should a parent neglect that step and make a payment or compose a correspondence then it will go to the wrong school. If a payment is made to the wrong school, then the incorrectly paid school would have to refund this payment. This will allow the parent to make the payment to the correct school. There is a small cost with bank payments incurred by the school each time.

To reiterate, the school control who has access and can reset passwords. They can set the level of access which may be different to what another school has set. If a parent is using the same email for each portal when they have children at different schools, they must select the correct school on login.

Finally, if a parent is experiencing an issue with the Parent Portal APP, check that they are accessing the correct school and if they are and there is a problem they need to contact that school. If this is for a child at another school, then you will have to direct them to that school.

Guidance from Arbor:

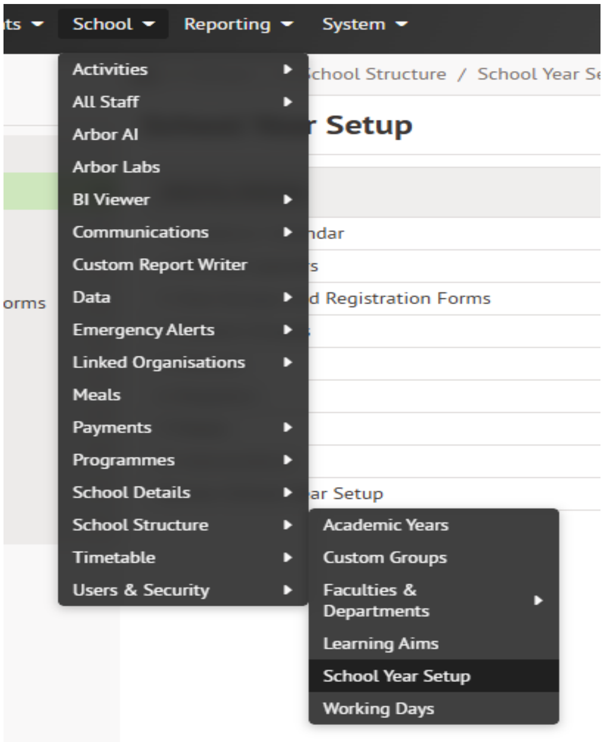
- Parent Portal and Parent App Checklist
- How can parents sign up for the Parent Portal or Parent App if they have a child at more than one school using Arbor?
- Managing the Parent Portal and App FAQ
- Common login issues with the Parent Portal - why can't parents log in?
- Log in as a guardian to Parent Portal

REMINDER OF END OF YEAR PROCESS

FAO Headteachers & Admin Staff

Just a reminder of the end of year process which should have been started by now.

This can be located from the following breadcrumb:
School > School Structure > School Year



There have been webinars that have covered this process, the links below will take you to these in Arbor HQ:

- https://arbor-hq.circle.so/c/resources/new-school-year-setup
- https://arbor-hq.circle.so/c/resources/new-school-year-setup-for-primaries-steps-6-9-9d6052
- https://arbor-hq.circle.so/c/resources/new-school-year-setup-for-secondaries-steps-6-9

The links above, steps 1 to 5 are common with both primaries and secondaries, steps 6 to 9 are also included but are aimed at the relevant school type.

Please log a call if you are experiencing issues or require assistance.

Please ensure that you have completed the end of year process before the start of the academic year as this will avoid issues.

SCHOOLS’ REPORTING REQUIREMENTS

The School’s Team is looking for feedback from our schools, on types of Reports they would like to create, or your most used reports

These reports could be from your previous MIS and is a report that you are looking to recreate within Arbor.

Are you in need of further assistance in creating a report, or maybe you have a report that you think other schools could also find helpful?

Please contact us by logging a call with the IT Service Desk on 01473 265555 or by email to ITServicedesk@suffolk.gov.uk, as we would like to consider the possibility of creating a shared resource area that all our Arbor schools can access.

REMINDER – ARBOR SUPPORT ARRANGEMENTS

FAO ALL SCHOOL STAFF

Schools should not contact Arbor directly for support.

Please remember to report all requests and incidents for Arbor MIS to the Suffolk County Council IT Service Desk.

This can be done by contacting us via 01473 265555 or emailing ITSrviceDesk@suffolk.gov.uk

If your call needs referring to Arbor for further support, this will be done by the team.

If your request relates to the Arbor finance system, please contact Schools’ choice via 0300 1231420 option 1 or email finance@schoolschoice.org

STUDENT UPNs

UPNs are generally issued upon entry to a state funded school, it is usually assigned when a child joins nursery class , or can be assigned at a later date when a child enters in to state funded school sector. There are only a few exceptions to this such as when the local authority advises that the UPN has already been allocated. It is expected that a UPN will remain with a pupil throughout their school career, although in some circumstances a new UPN may need to be issued where a child has been adopted or is at risk.

UPNs are used to facilitate the transfer of school-based education and attainment data through the state funded school system in England. The system enables accurate and timely data sharing between:

- schools
- local authorities
- central government

If you are having issues tracking down a UPN for new students, please feel free to log a call and we will be happy to assist, we can help find UPNs on the DFE national database on your behalf.

For anyone not familiar with adding UPNs to student profile on Arbor, please click on the below article, which explains, when UPN's can be assigned, adding new UPN's also how to assign UPNs in bulk, and permissions required.

Adding a UPN to a student – Arbor Help Centre

SCHOOL CYBER SECURITY UPDATE

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

Links to patching the vulnerabilities:

- APSB25-41 : Security update available for Adobe InCopy - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c0828486
- APSB25-48 : Security update available for Adobe Experience Manager - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c0828488
- APSB25-50 : Security update available for Adobe Commerce - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c082848a
- APSB25-53 : Security update available for Adobe InDesign - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c082848c
- APSB25-55 : Security update available for Adobe Substance 3D Sampler - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c082848e
- APSB25-57 : Security update available for Adobe Acrobat Reader - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c0828490
- APSB25-58 : Security update available for Adobe Substance 3D Painter - https://t-info.mail.adobe.com/r/?id=t1e8da1dc,ffd3da47,c0828495

Vulnerabilities

Adobe Security Bulletin:

APSB25-41 : Security update available for Adobe InCopy
APSB25-48 : Security update available for Adobe Experience Manager
APSB25-50 : Security update available for Adobe Commerce
APSB25-53 : Security update available for Adobe InDesign
APSB25-55 : Security update available for Adobe Substance 3D Sampler
APSB25-57 : Security update available for Adobe Acrobat Reader
APSB25-58 : Security update available for Adobe Substance 3D Painter

Threats landscape

Microsoft Patches 67 Vulnerabilities Including WEBDAV Zero-Day Exploited in the Wild

Microsoft has released patches to fix 67 security flaws, including one zero-day bug in Web Distributed Authoring and Versioning (WebDAV) that it said has come under active exploitation in the wild.

Of the 67 vulnerabilities, 11 are rated Critical and 56 are rated Important in severity. This includes 26 remote code execution flaws, 17 information disclosure flaws, and 14 privilege escalation flaws.

The patches are in addition to 13 shortcomings addressed by the company in its Chromium-based Edge browser since the release of last month's Patch Tuesday update.

The vulnerability that has been weaponized in real-world attacks concerns a remote code execution in WebDAV (CVE-2025-33053, CVSS score: 8.8) that can be triggered by deceiving users into clicking on a specially crafted URL.

The tech giant credited Check Point researchers Alexandra Gofman and David Driker for discovering and reporting the bug. It's worth mentioning that CVE-2025-33053 is the first zero-day vulnerability to be disclosed in the WebDAV standard.

Adobe Releases Patch Fixing 254 Vulnerabilities, Closing High-Severity Security Gaps

Adobe on Tuesday pushed security updates to address a total of 254 security flaws impacting its software products, a majority of which affect Experience Manager (AEM).

Of the 254 flaws, 225 reside in AEM, impacting AEM Cloud Service (CS) as well as all versions prior to and including 6.5.22. The issues have been resolved in AEM Cloud Service Release 2025.5 and version 6.5.23.

"Successful exploitation of these vulnerabilities could result in arbitrary code execution, privilege escalation, and security feature bypass," Adobe said in an advisory.

Almost all the 225 vulnerabilities have been classified as cross-site scripting (XSS) vulnerabilities, specifically a mix of stored XSS and DOM-based XSS, that could be exploited to achieve arbitrary code execution.

Security Tip of the month

Check URLs carefully to avoid phishing websites.

SCHOOLS EMAIL – MULTI FACTOR AUTHENTICATION & SELF-SERVICE PASSWORD RESET REGISTRATION

An email has been sent to all Schools' Email users asking them to register and set up Multi-Factor Authentication (MFA) and Self-Service Password Reset Registration (SSPR).

These measures will significantly enhance the protection of sensitive information and reduce the risk of unauthorised access on the School Email Platform.

Users should not need their mobile phone each time they try to log in. The system uses Microsoft's a risk-based access. Various indicators are used to determine if the person trying to log on needs to be challenged for MFA. The platform will learn what "normal" activity looks like and then not prompt for MFA. So, if you are using email from the School's Network and on your usual device then MFA should not be required, however if you try to connect from home or from an unfamiliar location then you will.

Several schools have fed back that they have policies around mobile phones, so we are hoping to get a balance of security without over prompting for MFA.

Please encourage your Email users to follow the instructions and report back any issues.

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