Suffolk
County Council

Schools’ IT Newsletter

JANUARY 2025

Included in this month’s issue:

Happy New Year!

The Schools’ IT Team would like to wish all our colleagues a very happy new year and welcome you all back after what we hope was a peaceful and restful break.

We look forward to continuing to offer support with your IT Services for 2025.

SPRING CENSUS 2025

Thursday 16th January 2025 will be Spring Census Day.

The Spring Census will require data on a specific period on census day which is guided by the last digit of the school DfE number.

Fileset so far is 2902 and is available to download via Anycomms and via the link below, however we are expecting fileset 2903 but this is not yet available. Please keep an eye on Anycomms for its' release:

https://customer.support-ess.com/csm?id=kb_article_view&sysparm_article=KB0056566&sys_kb_id=2ffa111a83a69294b20cc2c8beaad383&spa=1

Schools need to have applied the Autumn 2024 release of SIMS.net (7.220) to be able to complete a dry run.

Useful links:

- **ESS Handbooks**
- **DfE Guidance**
- **Census Newsfeeds**
- **Errors & Resolutions**
- **Link to DfE Class Information**.
- **Link to DfE Class Code**.

Other ways of obtaining useful information on any area in sims is to press the F1 key to retrieve the help info for that area.

For those schools who have already migrated to Arbor - please see the link below for information on preparing for this upcoming census:

https://support.arbor-education.com/hc/en-us/articles/360013361837-School-Census-Guide#h_01H9NBEF5NWQ4WJAY21M4T5K7F

Arbor will be holding a webinar on **8th January 2025 at 11am**, please see the following link on how to sign up:

https://support.arbor-education.com/hc/en-us/articles/360004772413-Upcoming-Webinars

The census line, (01473 260666), will be made available from:

Monday 13/01/2025 to Thursday the 16/01/2025 from 08:30 to 17:00.

Friday 17/01/2025 from 08:30 to 12:00.

House Keeping/Data Cleaning

For admin staff/Headteachers/technical staff

House keeping the sims database can generate improvements in read/write access. This also aids in migrations as the database is as lean as possible with the school only holding data it is required to do so. It should also be part of the schools GDPR policy to carry out these tasks and to not hold data they no longer need or have a right to hold.

Policy guidance on GDPR:

- https://www.gov.uk/data-protection
- https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

There is an attached crib sheet for the housekeeping but in essence, housekeeping in Sims .Net can be carried out over various tasks in sims:

- Delete Unwanted Persons
  - Tools | Housekeeping | Delete Unwanted Persons.
  - These are orphaned persons that have lost links to past records so can all be deleted.

- Delete Unwanted Contacts
  - Tools | Housekeeping | Delete Unwanted Contacts.
  - These are orphaned contacts that have lost links to past records so can all be deleted.

- Delete Admissions Applications
  - Tools | Housekeeping | Delete Admissions Applications.
  - These are admissions only that are being deleted, if you wish to delete the admitted record then this would have to be undertaken in bulk student deletion.

These tasks remove data from Sims .net; the other tasks retain the data but merge or highlight potential issues with the data.

Primary contacts can highlight missing data from the student details collectively.

The merge tasks, merge elements that may have been duplicated inadvertently in sims while maintaining any links entries.

Some of these processes are time consuming so the best practice is leaving the process to run when sims is not required.

Once there have been large numbers of changes to the sims database such as housekeeping, admissions, data collection, assessment, etc. It is worth running validate membership to resolve any issues with broken links with the data. This reduces the number of errors you can experience later accessing the data you have imported/changed in sims.

ARBOR FAQs FOR LA MAINTAINED SCHOOLS

How do I access the Arbor Help Centre?

The Arbor Help Centre can be accessed via the following link:

Arbor Help Centre

If you are having trouble locating the information you require, please do not struggle, just log a call via the IT Service Desk as normal, and one of the Schools IT Team will support you through your query.

How long will I have access to the Arbor Training Hub?

Users will have access to the training hub for 12 months from the account being created. If this is not your experience, please report this to the Schools IT Support team so we can liaise with the provider.

Who do I contact for support?

Please log MIS queries in the normal way via the ITServiceDesk@suffolk.gov.uk or call 01473 265555.

For Finance queries please contact Schools Choice via 0300 1231420 option 1.

To share feedback please email Andrew.brown2@suffolk.gov.uk or lizzie.winter@suffolk.gov.uk

SCHOOL CYBER SECURITY UPDATE

Date – 19/12/2024

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

Links to patching the vulnerabilities

- **CVE-2024-49138**
- **CVE-2024-35250**
- **CVE-2024-20767**
- **APSB24-69 :** Security update available for Adobe Experience Manager
- **APSB24-92 :** Security update available for Adobe Acrobat and Reader
- **APSB24-93 :** Security update available for Adobe Media Encoder
- **APSB24-94 :** Security update available for Adobe Illustrator
- **APSB24-95 :** Security update available for Adobe After Effects
- **APSB24-96 :** Security update available for Adobe Animate
- **APSB24-97 :** Security update available for Adobe InDesign
- **APSB24-98 :** Security update available for Adobe PDFL SDK
- **APSB24-99 :** Security update available for Adobe Connect
- **APSB24-100 :** Security update available for Adobe Substance 3D Sampler
- **APSB24-101 :** Security update available for Adobe Photoshop
- **APSB24-102 :** Security update available for Adobe Substance 3D Modeler
- **APSB24-103 :** Security update available for Adobe Bridge
- **APSB24-104 :** Security update available for Adobe Premiere Pro
- **APSB24-105 :** Security update available for Adobe Substance 3D Painter
- **APSB24-106 :** Security update available for Adobe FrameMaker

Vulnerabilities

CISA has added three new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- CVE-2024-49138 Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability
- CVE-2024-35250 Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability
- CVE-2024-20767 Adobe ColdFusion Improper Access Control Vulnerability

Adobe released security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

- **APSB24-69** : Security update available for Adobe Experience Manager
- **APSB24-92** : Security update available for Adobe Acrobat and Reader
- **APSB24-93** : Security update available for Adobe Media Encoder

- **APSB24-94** : Security update available for Adobe Illustrator
- **APSB24-95** : Security update available for Adobe After Effects
- **APSB24-96** : Security update available for Adobe Animate
- **APSB24-97** : Security update available for Adobe InDesign
- **APSB24-98** : Security update available for Adobe PDFL SDK
- **APSB24-99** : Security update available for Adobe Connect
- **APSB24-100** : Security update available for Adobe Substance 3D Sampler
- **APSB24-101** : Security update available for Adobe Photoshop
- **APSB24-102** : Security update available for Adobe Substance 3D Modeler
- **APSB24-103** : Security update available for Adobe Bridge
- **APSB24-104** : Security update available for Adobe Premiere Pro
- **APSB24-105** : Security update available for Adobe Substance 3D Painter
- **APSB24-106** : Security update available for Adobe FrameMaker

Threats landscape

Microsoft MFA AuthQuake Flaw Enabled Unlimited Brute-Force Attempts Without Alerts
Cybersecurity researchers have flagged a "critical" security vulnerability in Microsoft's multi-factor authentication (MFA) implementation that allows an attacker to trivially sidestep the protection and gain unauthorized access to a victim's account.
"The bypass was simple: it took around an hour to execute, required no user interaction and did not generate any notification or provide the account holder with any indication of trouble," Oasis Security researchers Elad Luz and Tal Hason said in a report shared with The Hacker News.
Following responsible disclosure, the issue – codenamed AuthQuake – was addressed by Microsoft in October 2024.

While the Windows maker supports various ways to authenticate users via MFA, one method involves entering a six-digit code from an authenticator app after supplying the credentials. Up to 10 consequent failed attempts are permitted for a single session.
The vulnerability identified by Oasis, at its core, concerns a lack of rate limit and an extended time interval when providing and validating these one-time codes, thereby allowing a malicious actor to rapidly spawn new sessions and enumerate all possible permutations of the code (i.e., one million) without even alerting the victim about the failed login attempts.

Security Tip of the month

Be Wary of Phishing Emails: Avoid clicking on suspicious links or attachments.

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