Suffolk County Council

Schools' IT Newsletter

FEBRUARY 2022

Included in this month's issue:

It is that time of year again for LA maintained schools to renew their IT Services for the forthcoming 2022 to 2023 year.

We are currently working in partnership with our 3rd party suppliers to ensure that we obtain the best prices for you.

We will be sending out your quotes over the coming weeks and would remind you that if you wish to give notice (N.B. notice periods apply, see website for details) on any of the services please do so in writing to schoolsitservices@suffolk.gov.uk

Hints and Tips on using SIMS InTouch

For Administrators, Data Managers or anyone with responsibility for Communicating with Parents

For those schools and academies using SIMS InTouch, ESS are hosting a Hints and Tips webinar on Wednesday 2nd March.

This webinar explores how SIMS InTouch can be used for communicating with staff, parents and students. Discover how SIMS InTouch can be incorporated into your workflows to improve communication around your school and between staff and parents.

Please use the following link to register for a place on this webinar, [Registration (gotowebinar.com)]

ESS / SIMS Clarity for the future update

Last month we provided an update on the changes proposed by ESS for the contractual arrangements for SIMs and SCC's position in relation to this. Following on from this we can advise that we will be meeting with ESS in the first week in February to discuss the proposed webinars. The aim of these is to give all schools an opportunity to hear directly from ESS on what they are proposing and the benefits they believe this will deliver for schools.

We are hoping that we will be able to run one or two webinars to give as many schools as possible the opportunity to raise any questions they may have. We are also planning to record one of these sessions and make this available to anyone who is unable to attend.

Once these sessions have been held, we will open a survey to obtain feedback and views from schools on the proposed changes. We need to be aware of procurement regulations and contractual arrangements but hope to be able to use the views provided by schools when considering how we proceed. Suffolk County Council currently has a contract with ESS to providing licensing for LA Maintained schools for SIMS and FMS. This contract is not due to expire until March 2025 and ESS have informed us that they intend to honour this.

Once we have confirmed arrangements for the webinars, we will contact all schools directly with details on how to join the sessions.

Spring School Census – Reminder for Academies

A reminder for all academies to log back into the DfE's COLLECT website and check the status of their Spring Census return. This will need to be repeated regularly until the Census becomes authorised.

We also recommend looking through both Duplicate Reports: Same UPN and Same Person Different UPN. Both reports can be run via the COLLECT website | Launch Reports… | select the report from the drop-down list and Launch Report. Please note that unresolved duplicates may have an impact on your schools funding and therefore all duplicates will need to be resolved before Wednesday 16th March 2022.

If you're an academy bought into the Remote SIMS Service and require further assistance, please call the IT Service Deck on 01473 265555

SCHOOLS' EMAIL SERVICE & PASSWORD RESETS

Thank you for using the forms on the SCC IT Website for raising requests for new email accounts, this has helped streamline the process and sped up the creation of new accounts.

Please do note that when the notification is received into your allocated secure mailbox when a new mailbox has been provisioned, there will be a request that staff members, in the first instance, create a Password Manager Account. This is to ensure that staff can reset their own password if they should forget it. Using password manager will enable users to reset their passwords without having to call the IT Service Desk, which we know can be frustrating at busy times.

We take identity management and access to your mail accounts seriously and follow industry standard best practice. This means that the IT Service Desk will seek to validate users requesting changes by asking for their payroll number. This process was designed when most schools purchased the SCC Payroll Service, as the school staff contracts were linked to their email accounts. While this is no longer the case, we still ask for payroll numbers for all staff needing an O365 email account to be set up, irrespective of where the payroll services are purchased, as this will be their Unique Identifier (UID). As noted above, the approach of using a UID is industry standard and like most on-line providers of mail accounts or on-line services.

The exception to this is Governor email accounts, agency and/or supply staff, as they generally do not have a payroll number. In these instances, we will now start providing a UID, which must be retained by that person should they need to contact us.

If a staff member calls the Service Desk for a password reset and they are unable to provide the UID, the Service Desk will not be able to carry out a reset. In these cases, we will need confirmation from the Headteacher regarding the person's identity by means of a telephone call on 01473 265555 or an email to ITServicedek@suffolk.gov.uk. This system is designed to ensure that only an authorised person has access to a school's mail account managed by SCC.

You can find more details about identity and access management in the National Cyber Security Centre's '10 Steps to Cyber Security' - **Identity and access management - NCSC.GOV.UK**

Changes to the schools' mail service – implementation of MFA

Following the launch of the Suffolk schools' cyber security service we have been reviewing the schools mail service and specifically arrangements around identity and access management. Due to previous concerns raised by schools, the current provision of the school's mail service does not have multi-factor authentication (MFA) - also known as two-factor authentication (2FA) - enabled. In the constant battle to ensure effective cyber and data security, it is no longer a viable approach to not enable MFA on schools' mail accounts. Enabling MFA will make accounts far more secure and aligns the solution with NCSC (National Cyber Security Centre) and DfE best practice & advice.

The DfE has recommended the use of authentication to protect on-line services:

Using authenticators to protect an online service - GOV.UK (www.gov.uk)

As has the National Cyber Security Centre:

Stepping up to multi-factor authentication - NCSC.GOV.UK

We are therefore working on a project to enable MFA on all schools' mail accounts. The project started at the beginning of the year and we have been working on the design and identified several schools to complete a proof of concept (POC) exercise with, before starting on a wider rollout to all schools. We will be looking to use Conditional Access to implement MFA which will enable us to have greater control on how the solution is implemented. This will be important as we are aware that schools use different methods of accessing their O365 mail accounts.

As the project progresses, we will be contacting and working with all schools in the service individually to ensure a smooth implementation of the service. We are aiming to complete the project by summer 2022.

Cyber Security – Distributed Denial of Service (DDoS) protection

All schools' broadband circuits managed by our telecoms partner, MLL Telecom, include Enterprise Grade DDoS protection. We know schools in Suffolk have been targeted by these types of attacks and thought it would be useful to provide some detail of what they are and how we take steps to prevent them.

What is a DDoS attack?

A volumetric Distributed Denial of Service (DDoS) attack is one of the most common forms of cyberattack. It is a malicious attempt to make an online service unavailable by flooding unwanted internet traffic from multiple sources, therefore making the online service or website unavailable.

Almost any type of internet-facing connected device could be a potential DDoS resource: Internet of Things (IoT) devices, smartphones, personal computers, and powerful servers. Simply put, a DDoS attack is like a traffic jam clogging up the motorway, preventing regular traffic from arriving at its desired destination.

How does an attack work?

For a DDoS attack to be successful, an attacker will spread malicious software to vulnerable computers, mainly through infected emails and attachments. This creates a network of infected machines called a botnet. Once the botnet has been established, the attacker is able to instruct and control the machines. Commands would be given to flood a site with traffic, causing the targeted server or network to overflow capacity, resulting in a denial-of-service to normal traffic.

The MLL Telecom Mitigation Service

The MLL DDoS mitigation service is powered by industry leading DDoS and Cyber Threat Protection Specialists Arbor Networks. The base offering is the "on demand" service which means that the service will be invoked as soon as an attack is detected.
The service constantly baselines traffic to ensure that only "out of baseline" spikes in traffic are classified as attack traffic. Once detected, the mitigation service removes the spurious traffic, sending only legitimate "clean" traffic back to the customer. The service protects against standard volumetric attacks, as well as so-called "low and slow" attacks that are designed to slowly deplete network resources and would otherwise go undetected.

If you want more details about Suffolk Cyber Security services, including the new Bronze level service please see: [Suffolk schools bronze cyber security service | Suffolk County Council]

Freshservice for schools

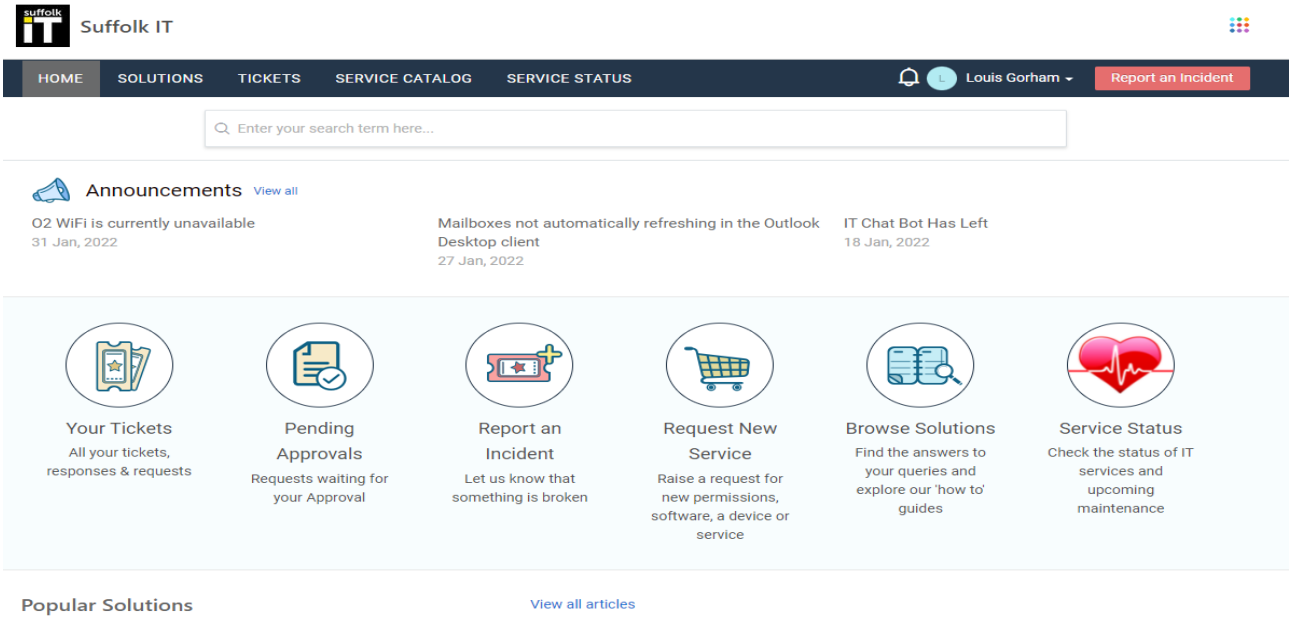
One of the issues schools regularly raise with us is how long it can sometimes take to contact us when they have a problem or wish to raise a request for a service. While calling us when you need immediate support remains the best option, we believe that providing access to our support portal will make it far easier for schools to contact us on most other occasions. Access to the SCC support portal will also enable schools to monitor the tickets they raise with us and check on updates and progress.

At SCC we use Freshservice (https://freshservice.com/) to manage all our IT support calls. We are currently working on opening this up by providing a portal that schools will be able to access to raise tickets. In doing this we will create a school specific instant which will enable users to access school services and provide full details of issues, enabling us to better allocate these and start work on resolving.

Benefits of using an on-line portal:

- Raise incidents and service requests at any time without the need of calling the Service Desk
- Update your own tickets – stops confusion when multiple tickets are raised for the same issue/request
- Check what progress we are making in resolving your issue or fulfilling your request
- Unique accounts for your school – each school will have unique named accounts to logon to the portal
- Central knowledge base of service information and help articles
- Live updates and announcements on service impacting issues

We are currently working on configuring the school's portal and once complete we will be looking to test with several schools who take the schools mail service from us. We need to test in this way as school mail users will already have a unique account to logon to the portal. We hope to be able to launch the initial trial before Easter. If this is successful, we will start a wider rollout in the summer term.



HOW TO CONTACT US!

You should continue to raise all standard incidents and service requests via the IT Service Desk on 01473 265555 or via itservicedesk@suffolk.gov.uk, our offices are open 08:30-17:00, Monday-Friday.

We have set up a mailbox for non-standard queries, e.g. enquiring about a new service, please email us at Schoolsitservices@suffolk.gov.uk