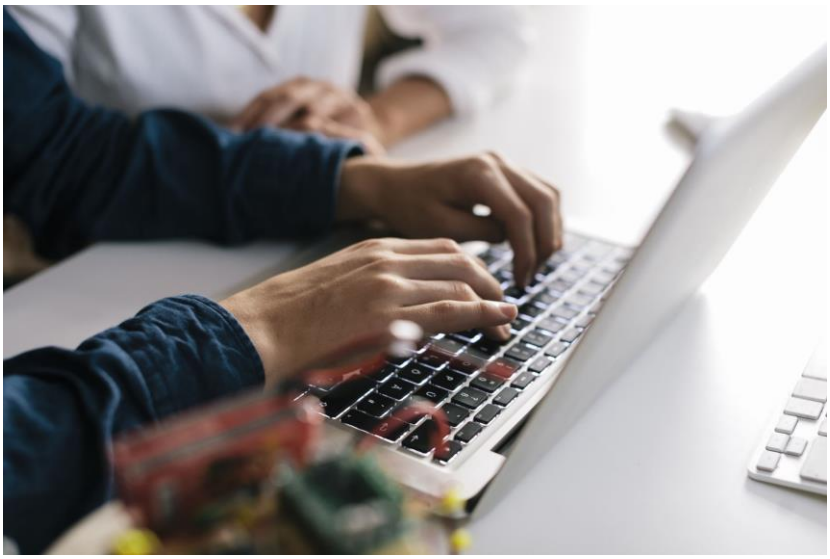
Suffolk County Council

Schools' IT Newsletter

FEBRUARY 2026

In This Issue



Email Security Spotlight

Are spoofed emails on the rise?
Yes — and schools are being targeted more than ever. Attackers are sending messages that look like they come from trusted staff, suppliers, or even the council.

What to watch for:
- **Odd or urgent requests**
- **Slightly altered email addresses**
- **Unexpected attachments or links**
- **External-email warnings on "internal" messages**

Quick tip:
Hover over the sender and any links before clicking. If something feels off, report it straight away.

Full article below

Arbor Updates & Upcoming Webinars

For Exams Officers, Attendance Officers & Admissions Officers

🗓️ February–March 2026 Webinar Series

Arbor is hosting a new round of webinars throughout **February and early March 2026**, designed to support colleagues working in **Exams**, **Attendance**, and **Admissions**.

View the full schedule and register: 🔗 ***https://arbor-hq.circle.so/c/webinars/***

If you can't attend live, all sessions will be recorded and uploaded afterwards to the **Arbor Resource Library**: 🔗 ***https://arbor-hq.circle.so/c/resources/***

⭐ Featured Webinar: Exam Entries

This session may be particularly valuable for those managing exam processes:
📝 ***Exam Entries | Arbor HQ***

Guidance on joining Arbor's free webinars is available here:
🔗 *How to join our free webinars – Arbor Help Centre*

🖥️ Additional Support & Resources

You can find details of the Arbor Service, including current FAQs, on the Schools' IT Services website:

🔗 ***Arbor Education – Suffolk County Council***

If you have a query that you cannot resolve using the resources above, please contact the IT Service Desk and log a ticket for further assistance.

🔔 Reminder for Schools Migrated to Arbor

It has come to our attention that some schools are missing **staff next-of-kin information** in Arbor. This data appears not to have transferred across from previous MIS systems during migration.

Please take a moment to review your staff records and ensure that **next-of-kin details are complete and up to date.**

This information is not included in the Workforce Census, so it will not be flagged automatically.

Thank you for your support in keeping staff records accurate.

🔧 Arbor Scheduled Maintenance

FAO all staff using Arbor

Please be aware of upcoming planned maintenance that will affect access to Arbor MIS.

🗓️ Date: Saturday 8 February 2026

⏰ Time: **11:00–14:00 GMT**

Arbor sites will be placed into **Maintenance Mode**, during which time they will **not** be available.

📌 Affected Services

- School MIS
- MAT MIS

Thank you in advance for your patience and understanding.

🧭 Tips for Admin Teams During the Downtime

- Plan any Arbor-dependent tasks (attendance checks, reports, data entry) before 11:00.
- Download any documents you may need access to during the maintenance window.
- Let colleagues know if you rely on Arbor for weekend work so they can plan around it.

Schools' Mail Service – Important Update

FAO school purchasing the Schools' Mail Service

As part of our ongoing work to maintain a secure and efficient Schools' Mail Service, all subscribing schools were issued a list of current users in September 2025 and asked to review and update the associated security details. This included confirming job titles, payroll numbers, and other essential verification information.

If your school has not yet returned this information, please ensure it is submitted as soon as possible. Without accurate and up-to-date records, the Service Desk is unable to complete mandatory security checks, meaning password reset requests cannot be processed.

MANDATORY USE OF UNIQUE IDENTIFIERS

Schools were previously advised to assign a unique identifier to any individual who does not have a payroll number, such as agency workers, temporary staff, or others not directly employed by the school. Although this requirement has not been enforced until now, it is now mandatory for all individuals who require a school mailbox, ***excluding governors***. Agency workers should have a unique reference number issued by their agency.

Each unique identifier must:

- **Be specific to the individual**
- **Not based on their date of birth**
- **Contain at least six digits**

Any request submitted without a valid unique identifier will be returned for correction, which may delay processing.

REQUESTS MUST COME FROM NAMED MAILBOXES

To support security and accountability, all requests ***must be submitted*** from a named mailbox rather than a generic or shared account. Requests sent from generic or shared mailboxes will be returned, resulting in further delays.

We appreciate your co-operation in helping us maintain a secure, compliant, and reliable service for all schools.

SCHOOLS' EMAIL SECURITY UPDATE

Schools Email Security Update

Protecting Your Inbox from Spoofing & Malicious Emails

Email remains one of the most common ways cybercriminals target schools. With high volumes of communication and busy staff, attackers often try to slip harmful messages into inboxes by pretending to be someone you trust. This month's update focuses on email spoofing and how to spot malicious attempts before they cause harm.

What Is Email Spoofing?

Email spoofing happens when a cybercriminal sends a message that looks like it comes from a trusted person—such as a headteacher, colleague, supplier, or even the local authority. Their goal is usually to trick staff into:

- Clicking a harmful link
- Opening a dangerous attachment
- Sharing sensitive information
- Making an urgent payment

These emails can be convincing, so awareness is essential.

Spoofing Alerts to Watch For:

1. Unusual or unexpected requests

If an email asks you to urgently buy gift cards, process a payment, or share personal data, treat it with caution.

2. Slightly altered email addresses

Attackers often change one character to make an address look legitimate:

- *headteacher@suffolk.sch.uk → headteacher@suff0lk-sch.uk*

3. External email warnings

If your system marks an email as external but it claims to be from someone inside the school or council, that is a red flag.

4. Pressure, urgency, or secrecy

Phrases like “I need this in the next 10 minutes” or “Don’t tell anyone yet” are common social-engineering tactics.

5. **Unexpected attachments or links**

Be cautious with invoices, safeguarding reports, or scanned documents you were not expecting.

🔍 How to Spot a Malicious Email:

Check the sender carefully.

Hover over the sender’s name to reveal the real email address. If it does not match the expected domain, stop.

Inspect links before clicking.

Hover over any link to see where it leads. If it looks odd or unrelated, do not click.

Look for spelling or grammar issues.

Many malicious emails contain unusual phrasing or formatting.

Trust your instincts

If the tone feels “off,” it probably is.

Verify using a separate method.

Call or speak to the person directly. Do not reply to the suspicious email.

🧰 What Schools Can Do Right Now:

- **Enable Multi-Factor Authentication (MFA)** for all staff accounts.
- **Use strong, unique passwords.**
- **Report suspicious emails immediately** to your IT support team.
- **Keep devices and browsers updated.**
- **Provide regular awareness reminders** to staff.

🏫 Why This Matters:

Schools hold sensitive data about pupils, staff, and families. A single malicious email can lead to data breaches, financial loss, and disruption to learning. Staying alert and following simple checks dramatically reduces risk.

Contacting the IT Service Desk

To help us support you quickly and efficiently, please use the correct contact routes for different types of enquiries.

Sales & New Service Enquiries

The Schools IT Services mailbox is intended for sales enquiries only and is monitored periodically.

For questions about new services, please email:

schoolsitservices@suffolk.gov.uk

Incidents & Service Requests

All standard issues, faults, and service requests must be logged via the IT Service Desk.

Using the correct route ensures your request is tracked and resolved without delay.

IT Service Desk Contact Options:

- Phone: 01473 265555
- Email: itservicedesk@suffolk.gov.uk

Requests sent to the wrong mailbox may result in delayed responses, so please ensure you use the correct contact method.

Office Hours

Our team is available:

Monday to Friday — 8:30am to 5:00pm