Suffolk
County Council

# Schools' IT Newsletter

SEPTEMBR 2025

## Included in this month's issue:

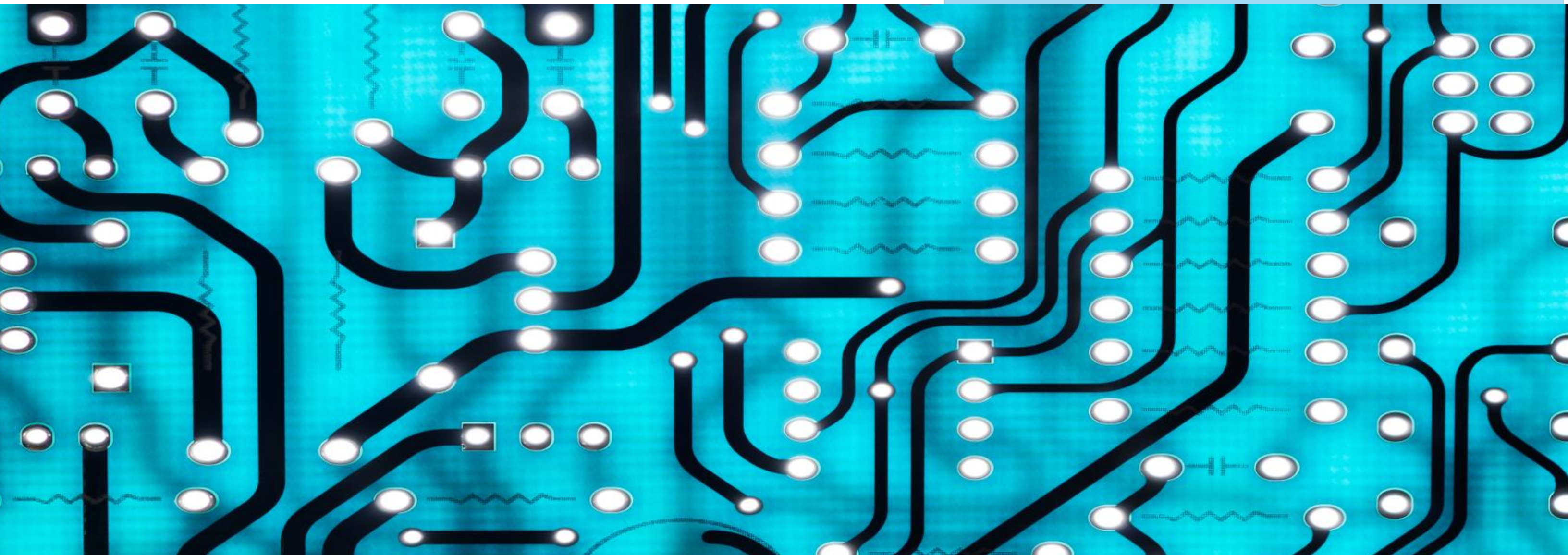
- **End of Year Process for 2024/2025**
- **Webinars or the new academic year 2025 to 2026**
- **Census dates for academic year 2025 to 2026**
- **Access to parent portal for leavers**
- **Notification of changes to schools' email service**
- **Cyber Security update**
- **IT Contact details**

***ACADEMIC YEAR 2025 TO 2026***

***SCC would like to welcome you all back from your summer break.***

***For those schools and academies that purchase the Schools' Email Service, please do take time to read the article on the changes that have taken place during the summer holiday, so that you are able to access your emails.***

***A reminder that for Arbor queries relating to the MIS please contact the IT Service Desk (details at the end of this newsletter) and for any finance queries you will need to contact Schools' choice on 0300 123 1420 or services@schoolschoice.org.***



# END OF YEAR PROCESS FOR 2024/2025 FAO ADMIN/HEADTEACHERS

For those that have not completed the end of year process for the academic year 2024 to 2025, the webinars are available to review for this process.

- 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

If the end of year process has not been completed, you may or may not have classes to enrol/place students into.  Also, may or may not have registers or meals available on the students first days.

Should this be the case then do remember that anything you setup needs to start from the beginning of the academic year.  If this does not start at the correct point, it could possibly cause some issues with the coming census points.

The webinars instructors also give guidance on material that can assist schools for these coming census points.

---

# WEBINARS FOR THE NEW ACADEMIC YEAR IN ARBOR

New academic year, new webinars to cover the basics and more in Arbor.

Webinars are a short instructional live format where you can ask questions on subjects that you book into.  A refresher of how to undertake some important tasks in Arbor after the summer break.

There are several webinars on numerous subjects and are replicated on a couple of days.  In this way, you should find something of use for the new academic year.

- Attendance and Meals.
  - 1st September 1330hrs to 1430hrs.
  - 3rd September 1000hrs to 1100hrs.
- Student Profiles and Enrolments.
  - 2nd September 1000hrs to 1100hrs.
  - 3rd September 1330hrs to 1430hrs.
- Logging in, Managing Permissions and Data Quality.

  - 1st September 1000hrs to 1100hrs.
  - 2nd September 1330hrs to 1430hrs.
- Clubs, Trips and Wraparound Care.
  - 4th September 1000hrs to 1100hrs.
  - 5th September 1330hrs to 1430hrs.

  - 11th September 1000hrs to 1100hrs.
  - 11th September 1330hrs to 1430hrs.
- Payments.
  - 4th September 1330hrs to 1430hrs.
  - 8th September 1000hrs to 1100hrs.
  - 12th September 1000hrs to 1100hrs.
  - 12th September 1330hrs to 1430hrs.
- Custom Report Writer.
  - 5th September 1000hrs to 1100hrs.
  - 8th September 1330hrs to 1430hrs.
- Reporting.
  - 10th September 1000hrs to 1100hrs.
  - 10th September 1330hrs to 1430hrs.
- Ask them Anything, Q&A.
  - 9th September 1000hrs to 1100hrs.
  - 9th September 1330hrs to 1430hrs.

They are spread over the first two weeks of September for schools' convenience.

https://arbor-hq.circle.so/c/webinars/

We would strongly recommend RSVP to these for guidance.  However, if you miss your desired webinar, you can obtain them from the Resource library afterwards.  Though, obviously, you cannot get a live response for questions.

# CENSUS DATES FOR ACADEMIC YEAR 2025 TO 2026

**Key Census Dates for the Diary:**

**Autumn census**

- census date – Thursday 2 October 2025
- LA Return Date – 10 October 2025
- DfE Deadline – Wednesday 29 October 2025

**Workforce census**

- census date – Thursday 6 November 2025
- LA Return Date – 14 November 2025
- DfE Deadline – Wednesday 5 December 2025

**Spring census**

- census date – Thursday 15 January 2026
- LA Return Date – 23 January 2026
- DfE Deadline – Wednesday 11 February 2026

**Summer census**

- census date – Thursday 21 May 2026
- LA Return Date – 29 May 2026
- DfE Deadline – Wednesday 17 June 2026

The LA return date is to allow for editing/resolutions to the census. To run reports to check for "duplicate UPN's" and "same person but different UPN". This is cross-checked against the entire UK.

Schools would have to make their own checks, for example FSM and UIFSM.

Please do not forget about the changes to the workforce census coming into effect next academic year. Guidance can be located from the May newsletter:

https://www.suffolk.gov.uk/business/it-services-for-schools-and-academies

Arbor release the dry run normally a week prior but notices will appear in Arbor HQ:

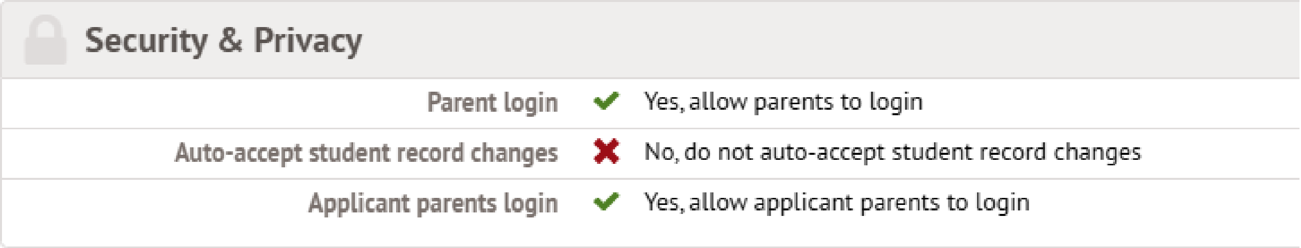
https://arbor-hq.circle.so/feed

# ACCESS TO PARENT PORTAL FOR LEAVERS

### FAO HEADTEACHERS/ADMIN

Access to Parent Portal is controlled at the school level, no one else can give or remove access other than the school.

So, once the school has opened access via the portal settings, all parents that had students active in this academic year can access the parent portal:
Students > Parents & Guardians > Parent Portal Settings



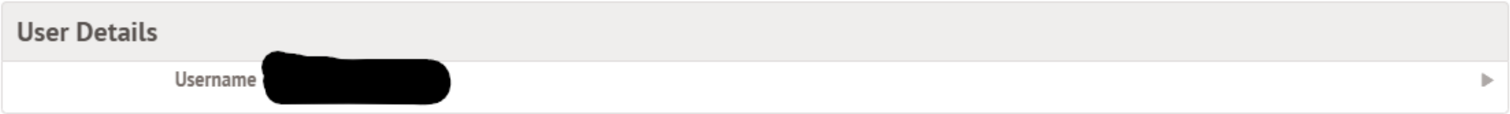
Security & Privacy

| | | |
|---|---|---|
| Parent login | ✓ | Yes, allow parents to login |
| Auto-accept student record changes | ✗ | No, do not auto-accept student record changes |
| Applicant parents login | ✓ | Yes, allow applicant parents to login |

Parent login controls access for parents that had a child that was a member of the school this academic year.  Applicant grants access to applicants who have not yet been enrolled on to the school.

This is an all or nothing setting, when enabled, all parents can then access the parent portal for this school if they are designated as the primary guardian.  When it is deactivated, it removes all parents' access.

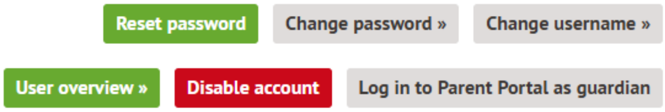
To control individual access, this needs to be controlled at the individual parent/guardian level.  In other words, go to the parent/guardian profile and enable this at the user



User Details

Username [redacted]

Click in this box on the parent/guardian profile page and then you can disable the access.



Further guidance is available on the link below:
Suspending/Disabling access for Parent Portal in Arbor

Difference between legal of primary guardian

To designate a primary/legal guardian you can do this from both the student profile and the guardian profile.  To do this from the student profile, click on the emergency contact for the guardian then select edit.  To do this from the guardian profile you would have to select the linked student in the linked students' box to update this information.

See frequently asked questions below:-

**What is a legal guardian?**

A legal guardian is a parent/guardian who are legally responsible for the child.  In other words, they may/may not have access to data for that child, but they are responsible for the child.  A legal guardian may have a court order against them and may have no/limited/full access to the child but are removed from portal access.

**They are the parent so must have parent portal access, shouldn't they?**

No, being designated the legal parent only, disconnects them from parent portal by design.  They can still put in a freedom of information request for data which the school decides how to process as they may have a court order against them that the school must follow.  However, this does not translate to being given parent portal access by default.  There may be other reasons why a legal guardian is not granted default access, so this is not an exhaustive subject.

**What is a primary guardian?**

This is a parent/guardian who will be granted access to the portal.  However, they should also be a legal guardian.  Arbor does not stop someone being designated as a primary guardian and not a legal guardian.

This is how some schools have worked around the issue of granting access to a guardian i.e. grandparents, while their legal parents are aboard working.  A relative can have parental responsibility while not being the legal guardian.

**How does Arbor classify as a child having been enrolled in an academic year?**

Technically, in Arbor, the end of year is concluded on the 31st of August, and a new academic year starts on the 1st of September.  For a child to be added to that class or year, they are "enrolled" in that year/class.  So, by terminology of Arbor, they are enrolled when they are added to a year/classroom group.

**When I turn on the portal, who has access to it?**

The following parents or guardians who are designated as a primary guardian will be granted access to the portal:

- The parent or guardian is on the Arbor system.
- The parent or guardian is linked to a child who is enrolled in a year/class this academic year.
- The child has been enrolled at the school and is not a leaver.

**Why is access controlled by the school and not the local authority or Arbor?**

This cannot be controlled by the other entities as they are not the data owners.  Therefore, this can only be under the authority of the school to enable the portal and to control access.

**Why are leavers of this academic year still allowed access to data via the portal?**

There may be a need for the parent/guardian to further communicate to the school.  For example, to pay off outstanding debts via the portal, so the parent/guardian can complete tasks as set by school admin or teachers, etc.

**Will past leavers from other academic years be able to access the Parent Portal?**

No, only parents or guardians of pupils that enrolled in this academic year will have access if the school has enabled the portal access.  As defined in the previous questions.

**Parents claim they can login, but I have not enabled the portal access, why?**

This is only partially true, providing the following criteria are met in full:

- The school uses Arbor MIS.
- The child was enrolled at the school this academic year.
- The username matches in both schools; this is usually the home email address of the parent/guardian.

If the above is met, then they will see the school's name in the drop down.  They, of course, will not have a password but they can reset it online.  They then can login but if the school has not enabled the parent portal it will be a blank screen.  Absolutely no data is visible, and they cannot communicate or interact with the portal at all.  However, they have logged in and this is all they can do but some schools have expressed concern that they are able to do this.  However, to reiterate, they have no access to data, and no interactions so is not a data breach.

**Parents have mentioned that they cannot login to the parent portal, but the child has left, what can I do?**

If they are trying to access the portal for the other school, then you should do nothing.  This is the other school's issue to resolve as they are active on their MIS.  This makes the other school the data owner of where they currently are and they control that access.  You cannot log a call for the parent to resolve an issue with another school.  Tell them to communicate the issue with the other school, as they alone can resolve it.

# NOTIFICATION OF CHANGES TO SCHOOLS EMAIL SERVICE

### What is changing?

Starting from 1 September 2025, we are introducing Multifactor Authentication (MFA) for all Email accounts managed by Suffolk County Council. Additionally, a new system will be implemented for resetting your Email account password.

### What is MFA?

Multifactor Authentication (MFA) is a security measure that requires multiple methods of authentication to verify a user's identity. This layered approach enhances security by ensuring that even if one authentication factor is compromised, unauthorized access is significantly reduced. To log in to your email, you will need to enter a password and use the Microsoft Authenticator phone app for the second level of authentication.

### How will this impact Email users?

When you log in to your email account from a school site, you ***should not*** be prompted for MFA, as the system is configured to recognise your schools IP address.

However, if you log in from outside a school site (e.g., at home), after entering your password, you will be prompted to check your Microsoft Authenticator app and enter a number shown on the device you are using to access your email account.

### What will be the system to reset my password?

As part of these changes, we have also introduced a new Self-Service Password Reset platform. When setting up your MFA for the Email Service, you will also need to use this platform. If you ever need to reset your password, you will use the Microsoft Authenticator phone app as part of the process.

### New request forms

As part of these changes, there are new forms on our website for you to request new mailboxes, delete a mailbox or to request assistance with the password on mailbox. Please do not save these forms to your own device as they are updated on a regular basis.

Please note that these forms MUST be completed and sent from a named mailbox of the head, bursar or business manager for them to be accepted by the SCC IT Service Desk.

# SCHOOL CYBER SECURITY UPDATE

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

**Links to patching the vulnerabilities:**

- APSB25-82 - https://t-info.mail.adobe.com/r/?id=t6ad2e2b5,80ec1a8e,c0a40dae
- Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise_xss_acc_cont-YsR4uT4U
- Cisco Webex Meeting Client Join Certificate Validation Vulnerability - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-join-yNXfqHk4

**Vulnerabilities**

**APSB25-82** : Security update available for Adobe AEM Forms

Originally posted: August 5, 2025

Summary: Adobe has released a security update for Adobe Experience Manager Forms on Java Enterprise Edition (JEE). This update addresses critical vulnerabilities that could lead to arbitrary code execution and arbitrary file system read. Adobe is aware that CVE-2025-54253 and CVE-2025-54254 have a publicly available proof-of-concept. Adobe is not aware of these issues being exploited in the wild.

Learn more: https://t-info.mail.adobe.com/r/?id=t6ad2e2b5,80ec1a8e,c0a40dae

1) Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities

CVE-2025-20331, CVE-2025-20332

SIR: Medium

CVSS Score v(3.1): 5.4

URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise_xss_acc_cont-YsR4uT4U ["https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise_xss_acc_cont-YsR4uT4U"]

2) Cisco Webex Meeting Client Join Certificate Validation Vulnerability

CVE-2025-20215

SIR: Medium

CVSS Score v(3.1): 5.4

URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-join-yNXfqHk4 ["https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-join-yNXfqHk4"]

**Threats landscape**

**Google's August Patch Fixes Two Qualcomm Vulnerabilities Exploited in the Wild**

Google has released security updates to address multiple security flaws in Android, including fixes for two Qualcomm bugs that were flagged as actively exploited in the wild.

The vulnerabilities include CVE-2025-21479 (CVSS score: 8.6) and CVE-2025-27038 (CVSS score: 7.5), both of which were disclosed alongside CVE-2025-21480 (CVSS score: 8.6), by the chipmaker back in June 2025.

CVE-2025-21479 relates to an incorrect authorization vulnerability in the Graphics component that could lead to memory corruption due to unauthorized command execution in GPU microcode.

CVE-2025-27038, on the other hand, use-after-free vulnerability in the Graphics component that could result in memory corruption while rendering graphics using Adreno GPU drivers in Chrome.

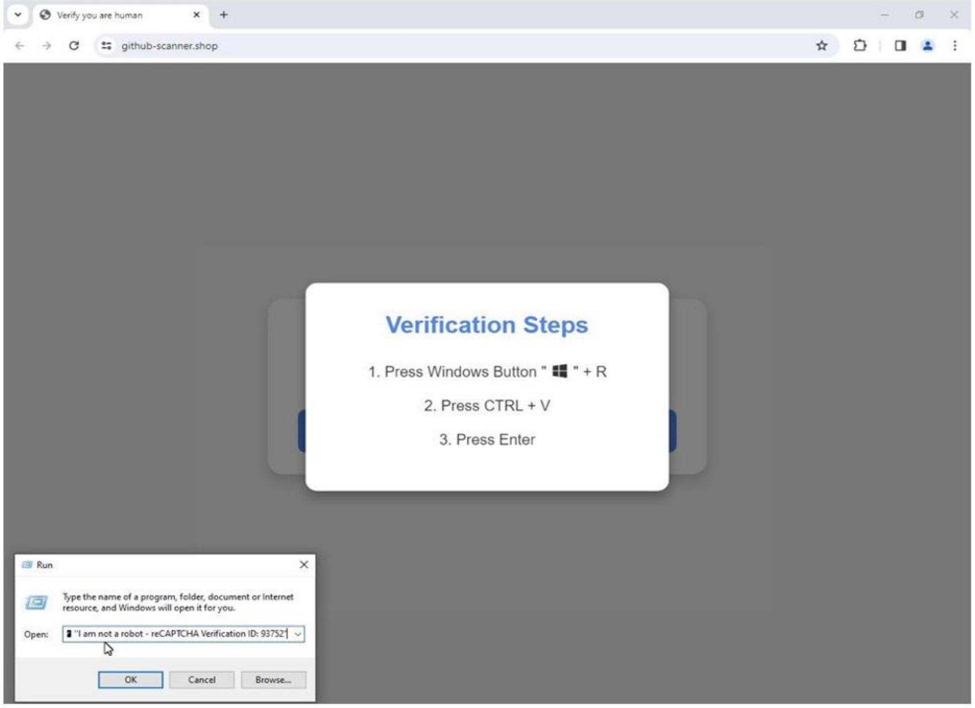
There are still no details on how these shortcomings have been weaponized in real-world attacks, but Qualcomm noted at the time that "there are indications from Google Threat Analysis Group that CVE-2025-21479, CVE-2025-21480, CVE-2025-27038 may be under limited, targeted exploitation."

Given that similar flaws in Qualcomm chipsets have been exploited by commercial spyware vendors like Variston and Cy4Gate in the past, it's suspected that the aforementioned shortcomings may also have been abused in a similar context.

**Security Tip of the month**

Never share your passwords with anyone

## “Clickfix”



Verification Steps

1. Press Windows Button " ⊞ " + R

2. Press CTRL + V

3. Press Enter

Run

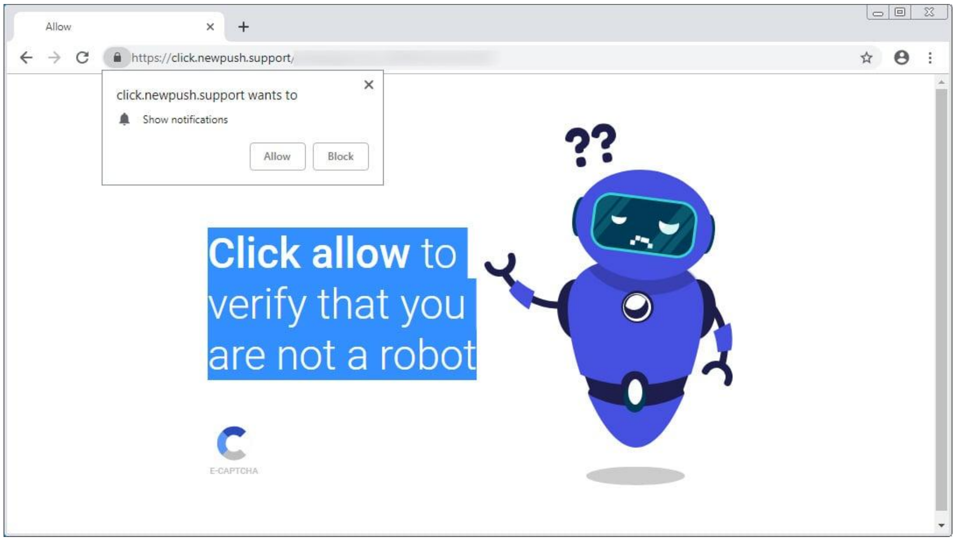
Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: "I am not a robot - reCAPTCHA Verification ID: 93752"

### Security Alert: Malicious Website Verification Prompts

We’ve identified a scam tactic where websites ask visitors to complete “verification steps” (e.g., proving you're not a robot) and then instruct them to press **Windows + R**, followed by **Ctrl + V** and **Enter**. These steps can trigger the download of malicious payloads, potentially compromising your device and data.

### “Allow Notifications Attack”



click.newpush.support wants to

Show notifications

Click allow to verify that you are not a robot

**Security Advisory: Avoid Enabling Suspicious Website Notifications**

Please do not enable notifications from websites that prompt you to "verify you are not a robot." These prompts can be deceptive and may lead to fake notifications claiming to be antivirus alerts or malware detections. Clicking on these can redirect you to scam pages designed to steal personal information or install harmful software.

If you encounter such prompts, close the page immediately and do not interact with it.

Stay safe online—thank you for your vigilance.

**Google Chrome: Remove Website Notification Permissions**

1. Open **Chrome**.
2. Click the **three dots** (⋮) in the top-right corner and select **Settings**.
3. In the left-hand menu, click **Privacy and security**.
4. Select **Site settings**.
5. Scroll down and click **Notifications**.
6. Under **Allowed to send notifications**, find the website you want to remove.
7. Click the **three dots** next to the site and select **Remove** or **Block**.

**Microsoft Edge: Remove Website Notification Permissions**

1. Open **Edge**.
2. Click the **three dots** (⋮) in the top-right corner and select **Settings**.
3. In the left-hand menu, click **Cookies and site permissions**.
4. Scroll down and select **Notifications**.
5. Under **Allow**, find the website you want to remove.
6. Click the **three dots** next to the site and choose **Remove** or **Block**.

# 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