

## CPOMS Authenticator – Trouble Shooting

If the **CPOMS Authenticator** app on your device reverts to 'Scan QR' code  
Or  
You have got a new device/ phone



If you still have access to the previous device, log-in with your usual app and skip to 'User steps to take' on page 2 to add your new device/phone.

Before you can setup the CPOMS Authenticator app on your new device, the previous device(s) needs to be removed by another **CPOMS Admin Key Holder** in school. This would usually be a member of your SLT/ Safeguarding team.



If there is not another Admin user available to remove your key

Or

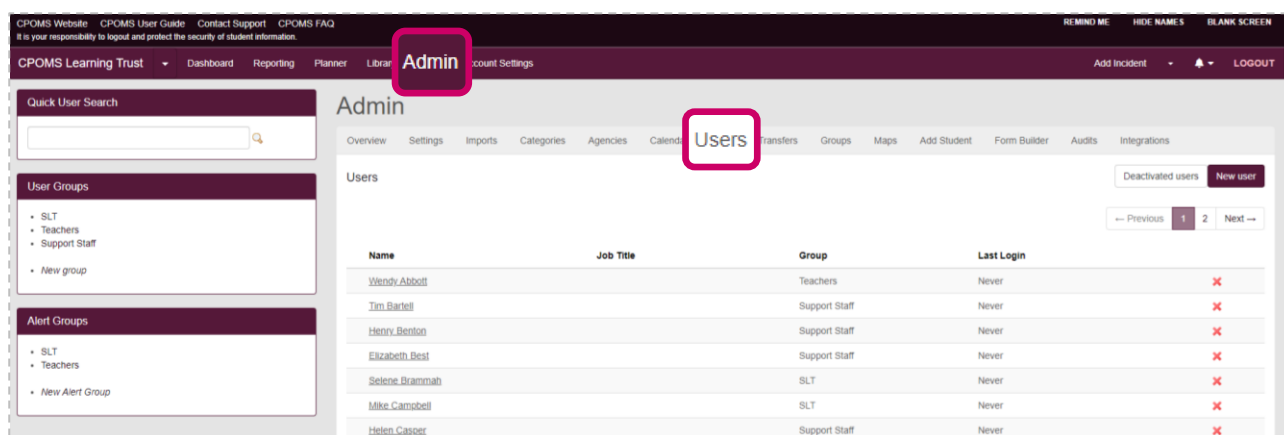
You are a Single Sign On (SSO) User - At present, if you are an SSO user we would need to remove the key at our side.

In the above cases, please email us at [support@cpoms.co.uk](mailto:support@cpoms.co.uk) from your school email address to request the key removal and we can arrange this for you.

The **Admin Key Holder** can easily remove your key in the following way, if you can please share the below instructions with them.

### Admin steps to take:-

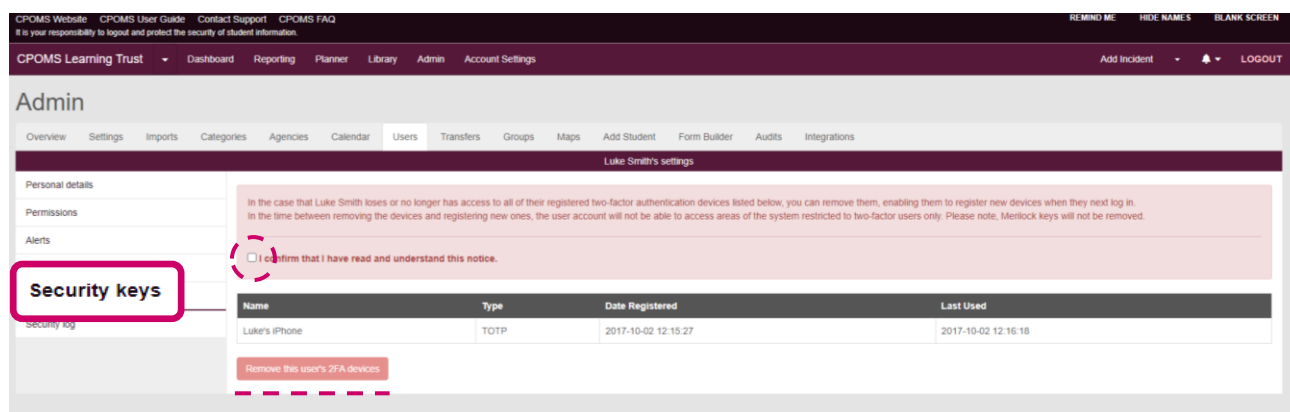
Go to 'Admin' and click on the 'Users' tab.



Name	Job Title	Group	Last Login
Wendy Abbott		Teachers	Never
Tim Bartlett		Support Staff	Never
Henry Benton		Support Staff	Never
Elizabeth Best		Support Staff	Never
Selene Brammah		SLT	Never
Mike Campbell		SLT	Never
Helen Casser		Support Staff	Never

Locate and click on the name of the person who requires their key removing from your user list. There is a 'Quick User Search' to the top-left corner of this tab if you have many users.

Now in their profile, click on **'Security Keys'** to the left.



CPOMS Website CPOMS User Guide Contact Support CPOMS FAQ  
It is your responsibility to log out and protect the security of student information.

CPOMS Learning Trust Dashboard Reporting Planner Library Admin Account Settings Add Incident LOGOUT

Admin

Overview Settings Imports Categories Agencies Calendar Users Transfers Groups Maps Add Student Form Builder Audits Integrations

Luke Smith's settings

Personal details

Permissions

Alerts

**Security keys**

Security log

In the case that Luke Smith loses or no longer has access to all of their registered two-factor authentication devices listed below, you can remove them, enabling them to register new devices when they next log in. In the time between removing the devices and registering new ones, the user account will not be able to access areas of the system restricted to two-factor users only. Please note, Meritlock keys will not be removed.

☐ I confirm that I have read and understand this notice.

Name	Type	Date Registered	Last Used
Luke's iPhone	TOTP	2017-10-02 12:15:27	2017-10-02 12:16:18

Remove this user's 2FA devices

If you are happy to continue and remove their key, tick the check box **'I confirm that I have read and understand this notice'** and click on the red **'Remove this user's 2FA devices'** to finalise.

The system will then confirm that you have successfully removed the device(s).

## User steps to take:-

Once your previous key(s) has been successfully removed, you can now add your new device/ set up your CPOMS Authenticator app again.



*If you are logged in to CPOMS already, please ensure you firstly **log out and back in to CPOMS again** before following the below instructions.*

## **Step 1:- Download the CPOMS Authenticator app**

For new devices, please download the CPOMS Authenticator app from your app store.

You can find the CPOMS Authenticator app by simply searching for the name in your app store, or by using one of the below hyperlinks:-



[Apple App Store](https://apps.apple.com/gb/app/cpoms-authenticator/id1093080934)

<https://apps.apple.com/gb/app/cpoms-authenticator/id1093080934>



[Google Play](https://play.google.com/store/apps/details?id=uk.co.meritec.cpomsauthenticator&hl=en_GB)

[https://play.google.com/store/apps/details?id=uk.co.meritec.cpomsauthenticator&hl=en\\_GB](https://play.google.com/store/apps/details?id=uk.co.meritec.cpomsauthenticator&hl=en_GB)

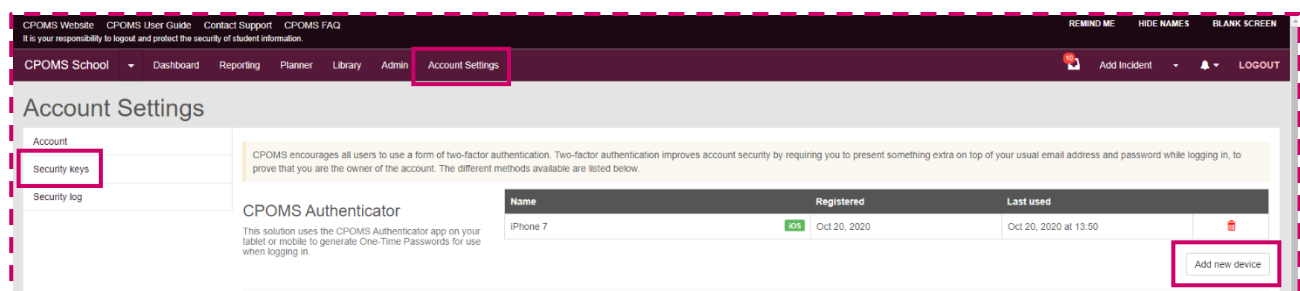
*If you have already downloaded the app, please skip to Step 2.*

## Step 2:- Log in to your CPOMS Account

Once you have downloaded the app, please log in to your CPOMS account, on a separate device to the one you have downloaded the app to. If you already have an existing key, please log in with it.

If you are using CPOMS for the first time, you will need to request an initial password to log-in firstly, by clicking on the **'Forgotten your password or using CPOMS for the first time?'** option, at your schools CPOMS login page, and following the simple steps.

Once you have logged in to CPOMS, click on the **'Account Settings'** section, along the top bar, and then click on the **'Security Keys'** tab, to the left-hand side of the screen. *Please see below screenshot.*



Under the sub-heading for **CPOMS Authenticator**, please click on **'Add new device'**.

This will then create a QR code for you to scan within your CPOMS Authenticator App.

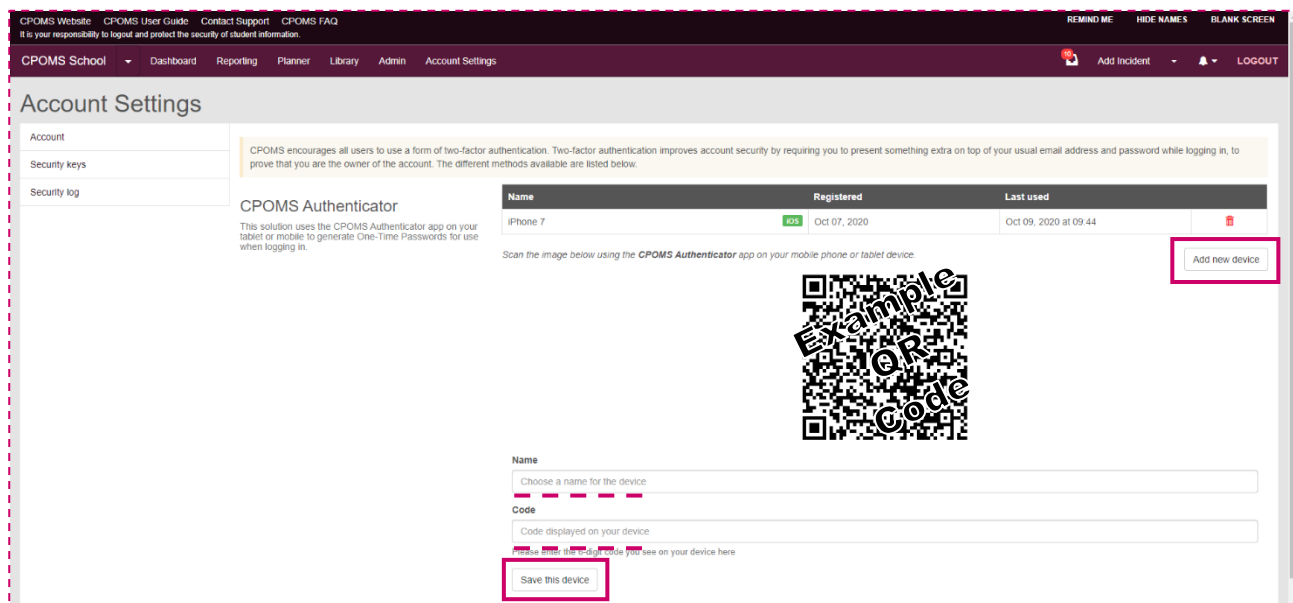
To scan the QR code, simply open up the app and tap the **'Scan QR Code'** message. Now point your device camera towards this image. Once the app has scanned the QR code, it will begin generating random numbers. *For security purposes, the numbers will change every 30 seconds as the circle goes round.*

**\*Please continue with the below points to ensure your app is setup correctly and saves to your account.**

Next, beneath the QR code image on screen, enter a **'Name'** for your device *i.e. iPad/ My Phone*.

In **'Code'** type in the current 6-digit code which is appearing in your app.

Lastly click **'Save this device'**.



CPOMS Website CPOMS User Guide Contact Support CPOMS FAQ

CPOMS School Dashboard Reporting Planner Library Admin Account Settings

Account Settings

Account

Security keys

Security log


CPOMS encourages all users to use a form of two-factor authentication. Two-factor authentication improves account security by requiring you to present something extra on top of your usual email address and password while logging in, to prove that you are the owner of the account. The different methods available are listed below.

CPOMS Authenticator

This solution uses the CPOMS Authenticator app on your tablet or mobile to generate One-Time Passwords for use when logging in.

Name	Registered	Last used
iPhone 7	Oct 07, 2020	Oct 09, 2020 at 09:44

Scan the image below using the CPOMS Authenticator app on your mobile phone or tablet device.



Add new device

Name

Choose a name for the device

Code

Code displayed on your device

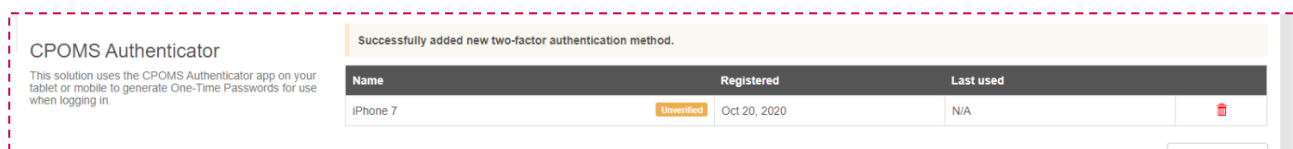
Press the Send Code button you see on your device here

Save this device

Once saved, your new Soft Key will appear listed in the CPOMS Authenticator section.

**Unverified**

*will appear next to its name until you use the app to login, this is nothing to worry about.*



CPOMS Authenticator

This solution uses the CPOMS Authenticator app on your tablet or mobile to generate One-Time Passwords for use when logging in.

Successfully added new two-factor authentication method.

Name	Registered	Last used
iPhone 7	Unverified Oct 20, 2020	N/A

### Step 3 - Elevate your Access

To elevate your access, please click on **'Dashboard'** to the top left-hand corner of the screen in CPOMS, to *refresh your page*. To the top right-hand corner of your CPOMS screen, you should now have a **'Elevate Your Access'** option to click on. Once selected, **enter the 6-digit number** appearing on your app currently, and click **'Authenticate'**. *If you are already logged in with a different key, the 'Elevate Your Access' option will not appear.*



CPOMS

Two Factor Authentication

CPOMS Authenticator Code

Open the CPOMS Authenticator app on your registered device and press Send Code, otherwise enter the code yourself if your device is not connected to the internet

Authenticate

If you are in a higher level user group, your access will now change to reflect your user group permissions.

When you log in to CPOMS in the future, your app will give you the option to 'approve' or 'deny' a log in, rather than typing in the code manually each time. Alongside this option, it will display the approximate location of where the login took place (based on the IP address), so you can easily differentiate whether it was you who initiated the login before you choose to click 'approve'.

## CPOMS Authenticator FAQs

### Error message 'Incorrect or out of date code'?

If you receive an error message which says 'Incorrect or out of date code', when logging in to CPOMS with your key, it means the date and time on the device of your app is out of sync with our servers (it may be slightly fast or slow).

Usually the way to fix this is to amend the date and time setting on the device of your app to 'set automatically'. This ensures the date and time is set identically to our servers.

### Error message 'No usable date' when trying to scan the QR code?

This sometimes occurs if you are trying to scan the QR code via the normal camera on your device, rather than through the CPOMS Authenticator App. To scan the QR code, please ensure you have firstly opened the CPOMS Authenticator App, and tapped 'Scan QR Code'. Please then point the camera toward the QR code image when prompted.

### My location on the app is not accurate?

The location shown on the app is actually taken from the location of your I.P address, so it can sometimes appear to be further afield.

To put your mind at rest you can check the location of your I.P address before choosing to 'approve'.

Simply search 'What's my IP' in a search engine (*i.e. Google*) on your app device and click on <https://whatismyipaddress.com>, which is usually the first result. This will then confirm the location of your I.P address, which you can check matches against the location shown in your app.

Or if you would prefer, you can choose to type in the numbers manually into CPOMS, rather than clicking on the approve option.

---

For further assistance on any of the above please do not hesitate to contact us on

**01756 797766** or [support@cpoms.co.uk](mailto:support@cpoms.co.uk).

