Multi-Factor Authentication (MFA) Registration

What is Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an extra layer of protection to your College Microsoft 365 account by requiring a second step to your authentication (logon) process.

This means if your account is compromised (for instance your password has been stolen) and your details are shared, it will be difficult to gain access to your college account. This protects yourself and the College's data.

Why are we enabling it?

We are enabling this for all College users to increase our protection from unauthorised access to our systems. This will help keep you and our data safe when using the College systems.

Educational institutions, particularly FE colleges and universities have been a big target in recent months, with realistic emails being sent to staff and students trying to “phish” for your username and password by inviting you to click on a link.

If your username and password are compromised (or stolen) a threat actor/hacker can get access to your account, and any of the data and systems you are given access to as part of your job, or any course you are studying. Without MFA, the username and password can be used without any additional notification to yourself.

We frequently receive reports of staff and student account login attempts from locations all over the world, even when the account holder is on site within the College.

With the additional level of verification provided by MFA we can reduce the impact of stolen usernames and passwords.

How will it work?

The first thing to do is to follow these instructions and set up your mobile phone as your authentication device. This mobile phone will then be used to allow you to sign in on any other device outside the College.

Once you have set up your mobile phone, every time you sign-in to your account on a non-College computer, you will get a request pop up on your mobile phone to approve this sign-in. Tapping the approve button will allow your sign-in to continue. You can choose to receive text message approval codes instead of a pop-up approval if you want.

You will not be prompted for this method when using a laptop you have been issued by the College, or if you are using a device on campus.

Staff MUST set up MFA at a college computer and/or connected to the college wireless.

Students need to be in the UK.

We highly recommend setting up the text/SMS method as well.

You don’t have to install the app. Just using the text/SMS method is fine.

Instructions are on page 3

Setting up a primary authentication method. What do I need to do?

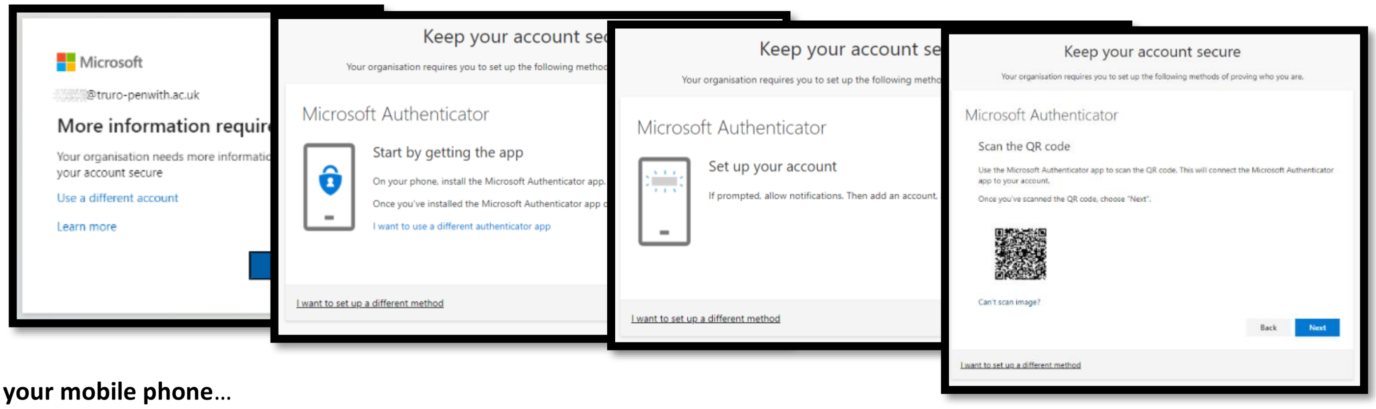
We highly recommend installing the Microsoft Authenticator App for your first authentication option.

We do not recommend use of the 'Office phone' option

Starting on your College desktop computer…

- Go to https://aka.ms/mfasetup/ And sign-in with your College email address. You will be prompted for more information.
- Follow the instructions for Microsoft Authenticator. You should end up with your computer dispalying a QR code, and your mobile phone asking to scan the code:

The Microsoft Authenticator app is completly free of charge. Beware of similar apps requiring a subscription.
The official Microsoft app for Android and Apple can be found at
https://www.microsoft.com/en-us/security/mobile-authenticator-app



Microsoft
[redacted]@truro-penwith.ac.uk
More information requir
Your organisation needs more informatio
your account secure
Use a different account
Learn more

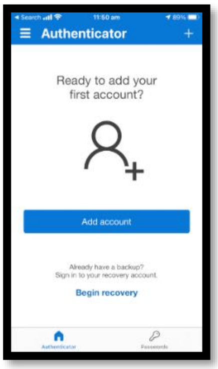
Keep your account sec
Your organisation requires you to set up the following method
Microsoft Authenticator
Start by getting the app
On your phone, install the Microsoft Authenticator app.
Once you've installed the Microsoft Authenticator app c
I want to use a different authenticator app
I want to set up a different method

Keep your account se
Your organisation requires you to set up the following metho
Microsoft Authenticator
Set up your account
If prompted, allow notifications. Then add an account.
I want to set up a different method

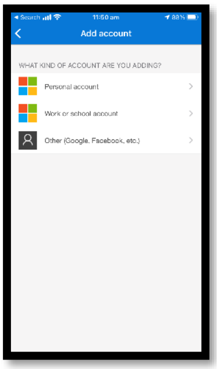
Keep your account secure
Your organisation requires you to set up the following methods of proving who you are.
Microsoft Authenticator
Scan the QR code
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app to your account.
Once you've scanned the QR code, choose "Next".
Can't scan image?
Back Next
I want to set up a different method

On your mobile phone…

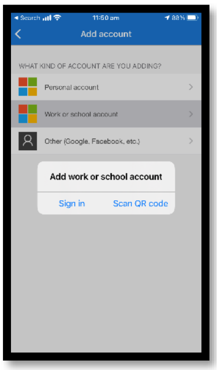
- Click on the **+** in the top right of the app,
- Click on 'Work or school account' and the Scan QR code option



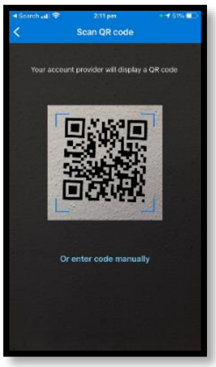
Authenticator
Ready to add your first account?
Add account
Already have a backup?
Sign in to your recovery account.
Begin recovery



Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)



Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)
Add work or school account
Sign in Scan QR code

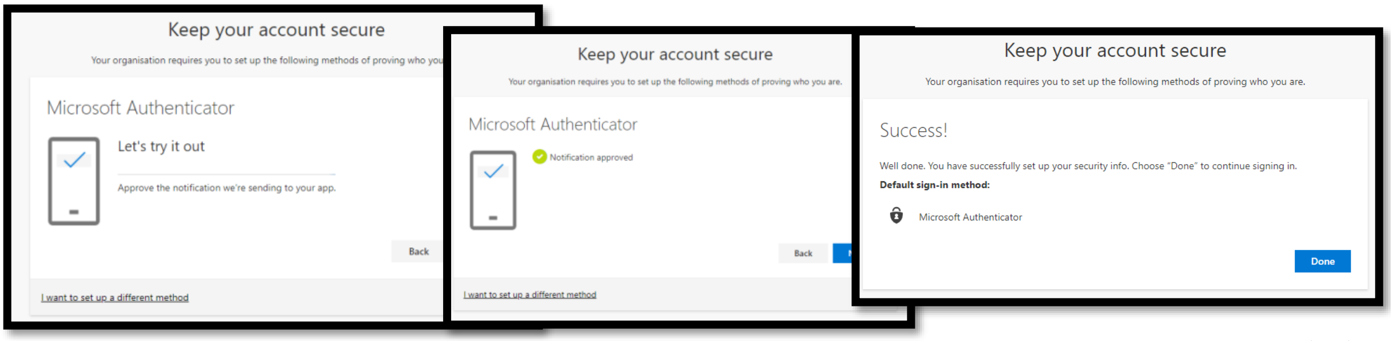


Scan QR code
Your account provider will display a QR code
Or enter code manually

- Use your mobile phone to scan the QR code on your computer screen.

Back to your College desktop computer…

- Your computer should now ask you to try it out by sending an approval request to your mobile. Once approved on your mobile, you will see the Success page. You're done setting this up!



Keep your account secure
Your organisation requires you to set up the following methods of proving who you
Microsoft Authenticator
Let's try it out
Approve the notification we're sending to your app.
Back
I want to set up a different method

Keep your account secure
Your organisation requires you to set up the following methods of proving who you are.
Microsoft Authenticator
Notification approved
Back
I want to set up a different method

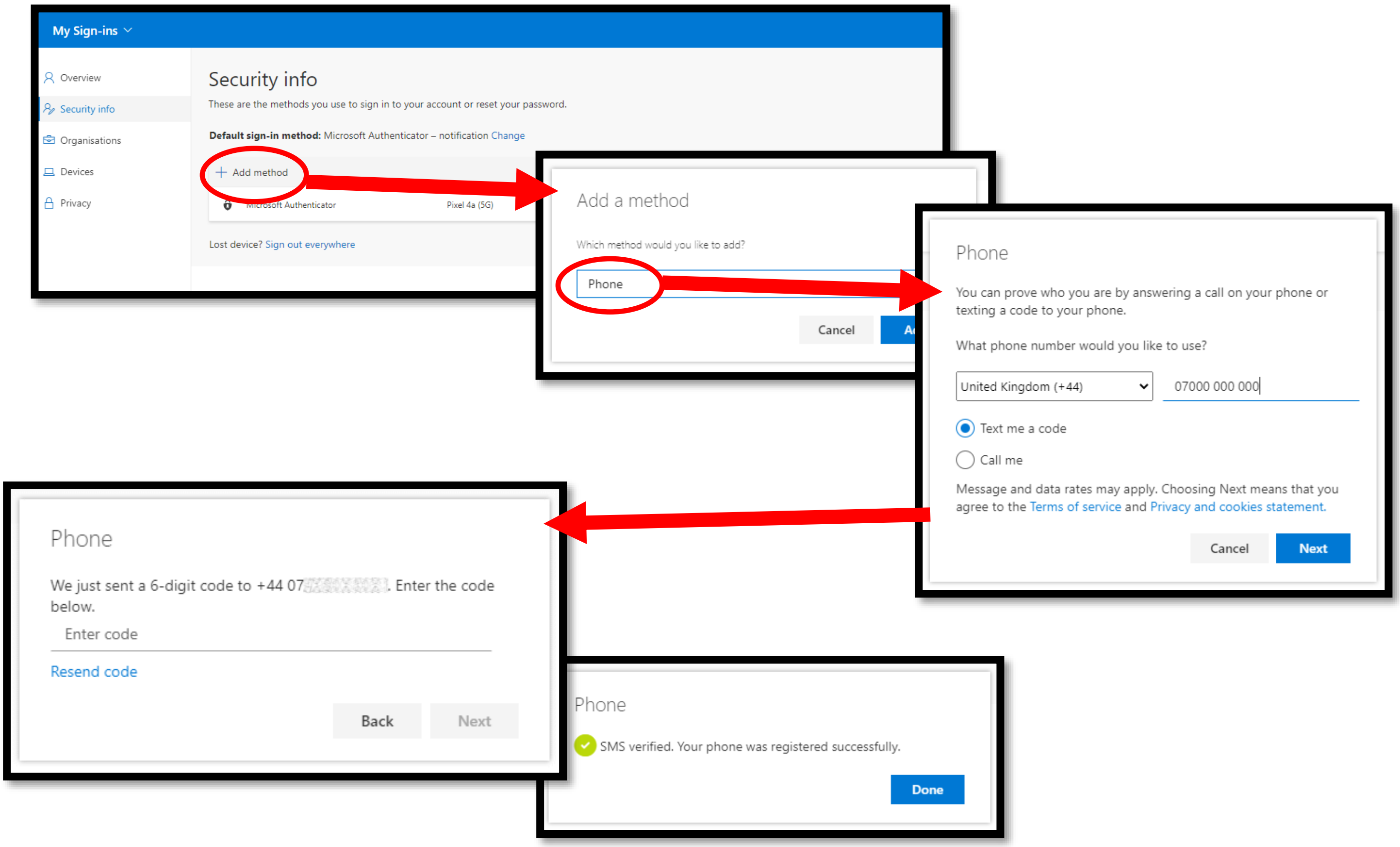
Keep your account secure
Your organisation requires you to set up the following methods of proving who you are.
Success!
Well done. You have successfully set up your security info. Choose "Done" to continue signing in.
Default sign-in method:
Microsoft Authenticator
Done

Set up a secondary authentication method.

We also highly recommend also setting up a mobile number against the account as well. To do this please follow the below instructions. This assumes you have already set up the primary method as above.

Note: We do not recommend use of the 'Office phone' option

- On a desktop computer, go to https://aka.ms/mfasetup/
- Click on, **+ Add method**, under Security info
- Select **Phone**
- Select **United Kingdom (+44)**, enter your mobile number, select **Text me a code**



My Sign-ins

Overview
Security info
Organisations
Devices
Privacy

Security info

These are the methods you use to sign in to your account or reset your password.

Default sign-in method: Microsoft Authenticator – notification Change

+ Add method

Microsoft Authenticator Pixel 4a (5G)

Lost device? Sign out everywhere

Add a method

Which method would you like to add?

Phone

Cancel Ad

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United Kingdom (+44) 07000 000 000

● Text me a code

○ Call me

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

Cancel Next

Phone

We just sent a 6-digit code to +44 07[redacted]. Enter the code below.

Enter code

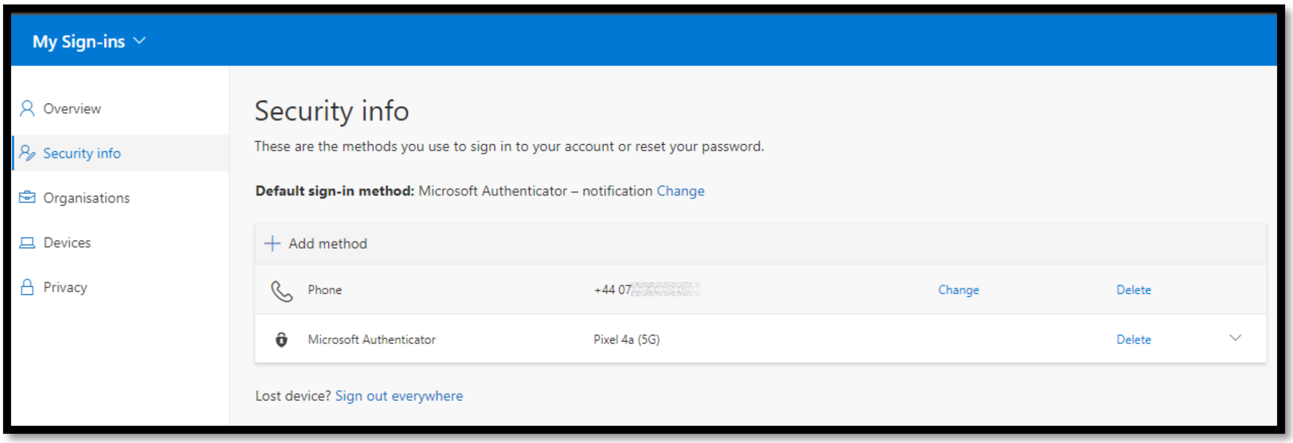
Resend code

Back Next

Phone

✓ SMS verified. Your phone was registered successfully.

Done



My Sign-ins

Overview
Security info
Organisations
Devices
Privacy

Security info

These are the methods you use to sign in to your account or reset your password.

Default sign-in method: Microsoft Authenticator – notification Change

+ Add method

Phone	+44 07[redacted]	Change	Delete
Microsoft Authenticator	Pixel 4a (5G)		Delete

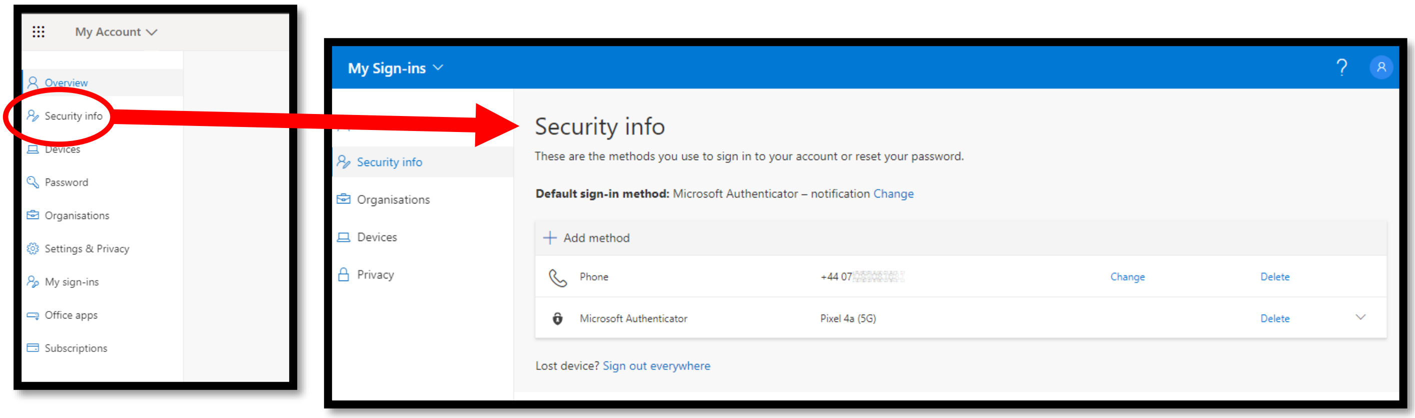
Lost device? Sign out everywhere

Multi-Factor Authentication (MFA) Registration

Updating your authentication methods later…

When you replace your mobile and/or mobile number. Please remember to update the information on your account.

- From a desktop computer, go to https://myaccount.microsoft.com/
- Click on **Security info**. This will list your current authentication methods with the option to **change**, **delete** or **add**.



Security info

These are the methods you use to sign in to your account or reset your password.

Default sign-in method: Microsoft Authenticator – notification Change

Phone	+44 07	Change	Delete
Microsoft Authenticator	Pixel 4a (5G)		Delete

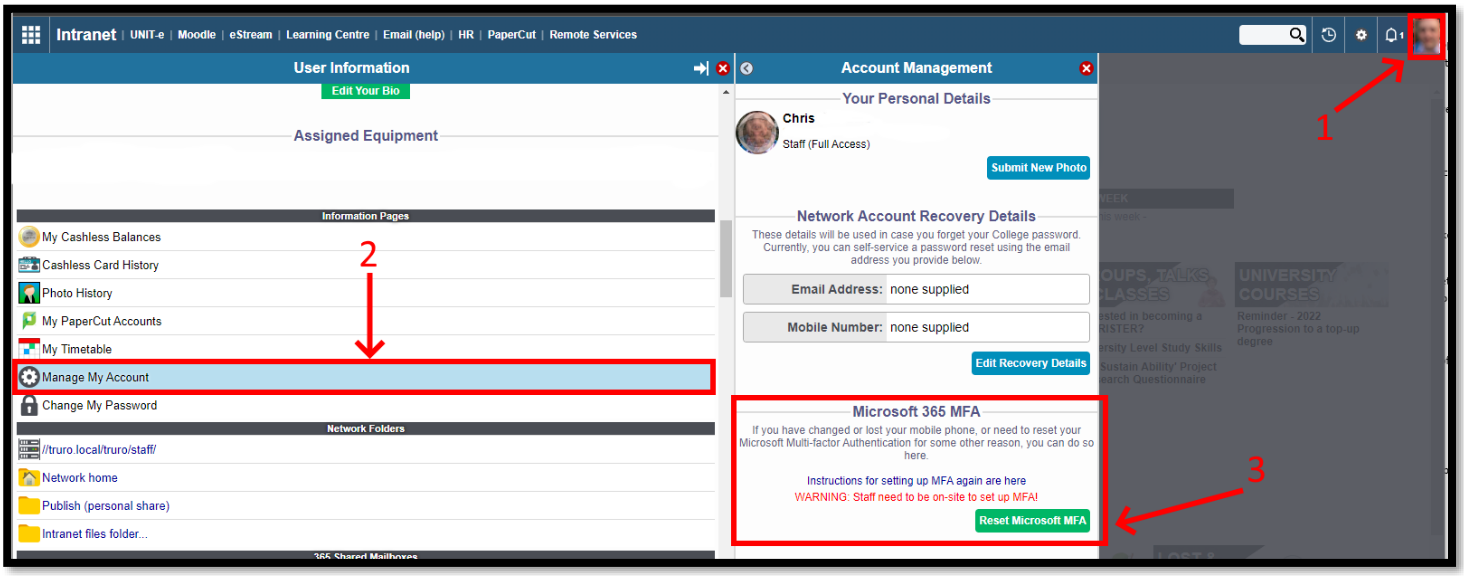
Lost device? Sign out everywhere

Resetting MFA on your account

If you've changed your phone and your account is still linked to your old device. You will need to reset MFA on your account by doing the following.

Remember: Staff must be on a college site to set up MFA again. Students need to be in the UK.

Go to the College Intranet (https://remote.truro-penwith.ac.uk) » Click on your profile photo in the top right » Click Manage my Account » Enter your password » Click the reset MFA button



Chris

Staff (Full Access)

These details will be used in case you forget your College password. Currently, you can self-service a password reset using the email address you provide below.

Email Address: none supplied

Mobile Number: none supplied

If you have changed or lost your mobile phone, or need to reset your Microsoft Multi-factor Authentication for some other reason, you can do so here.

Instructions for setting up MFA again are here

WARNING: Staff need to be on-site to set up MFA!

FAQs

Isn't this going to slow down the logging into a college computer?
No. When you are using a computer or device within the College, or using a remote College managed device, you will not be prompted to approve your log in with the app or verify with your mobile details.

Do I have to approve every log on to my private device?
No. For most applications that people connect to they will have the option to trust this device for 30 days and will therefore not be constantly prompted to MFA. However, some systems require additional security and therefore will prompt every time.

Do I have to do it?
Yes. Accounts are compromised every day, and we see a considerable number of sophisticated attempts get people to enter their credentials. Once your account details have been obtained by threat actors, your personal and College data is available to them. Multi-factor authentication helps to prevent access without also having access to personal device that you hold. Multi-factor authentication is not only recommended for businesses, but also highly recommended for all your personal accounts as well. Other companies such as Amazon, Apple, eBay, Google, and PayPal all recommend using MFA.

Is there another way other than using my personal device?
For the reasons described above, when accessing our services outside the college campus we *have* to put additional security measures in place. This is a condition of accessing College systems on private equipment and without MFA, we cannot provide access. Remember, this does not apply to any work devices you have been issued from the College.

I've lost my mobile/changed my number what do I do?
Please first follow the instructions under '**Resetting MFA on your account**' on the previous page. Still having issues? Please let us know on the Request and Support Centre on the intranet and we can reset your account. Once reset you will be able to re-register.

I've received an unexpected text message or an App notification.
This means someone has successfully logged into your account with your password. At this stage do NOT click approve in the App, instead you should immediately change your college password.

I use my private phone to check my emails, will MFA affect this?
Most email apps provide support for MFA so users will be prompted to MFA every 30 days. We recommend using Microsoft Outlook on personal devices.

Does this mean I've got to install Teams and/or Outlook on my mobile phone?
No. Your mobile phone will only be used to approve sign-ins on your other devices. The authenticator app is NOT linked to the College systems other than to give you a sign-in approval.

The authenticator app is only to allow you to approve your sign-ins outside the College. Once your mobile phone is set up as your authentication device, you can use Teams, Outlook, or OneDrive on your laptop, home computer, or tablet. Your mobile phone will receive a request to approve this sign-in and saying yes to this allows your other device access to your account.

My email app keeps on asking for authentication. How can I stop it.
This is due to some apps not fully supporting the MFA process. We strongly recommend installing the official Microsoft Outlook App. Search for **Outlook** in the App Store or Play Store. This is a FREE app.

Can students register MFA at home?
Yes, students can complete the process within the UK & Ireland. They do NOT need to be on site.

I have a Huawei mobile and the App doesn't work. What do I do?
Staff and students are reporting that the app doesn't work on some Huawei mobiles. This is due to the Play Store/Apps being restricted on some Huawei mobiles. Use the secondary (Text/SMS) method instead.