Enabling Two-Factor Authentication - Students

> ⚠️ **After being set up, if you receive an authentication request that you did not expect, report it to the IT Service who will change your password as soon as possible.**

Setting Up

When attempting to log in to your Microsoft account off-site, via a mobile device or a desktop or laptop, after entering your password you will see the following message:
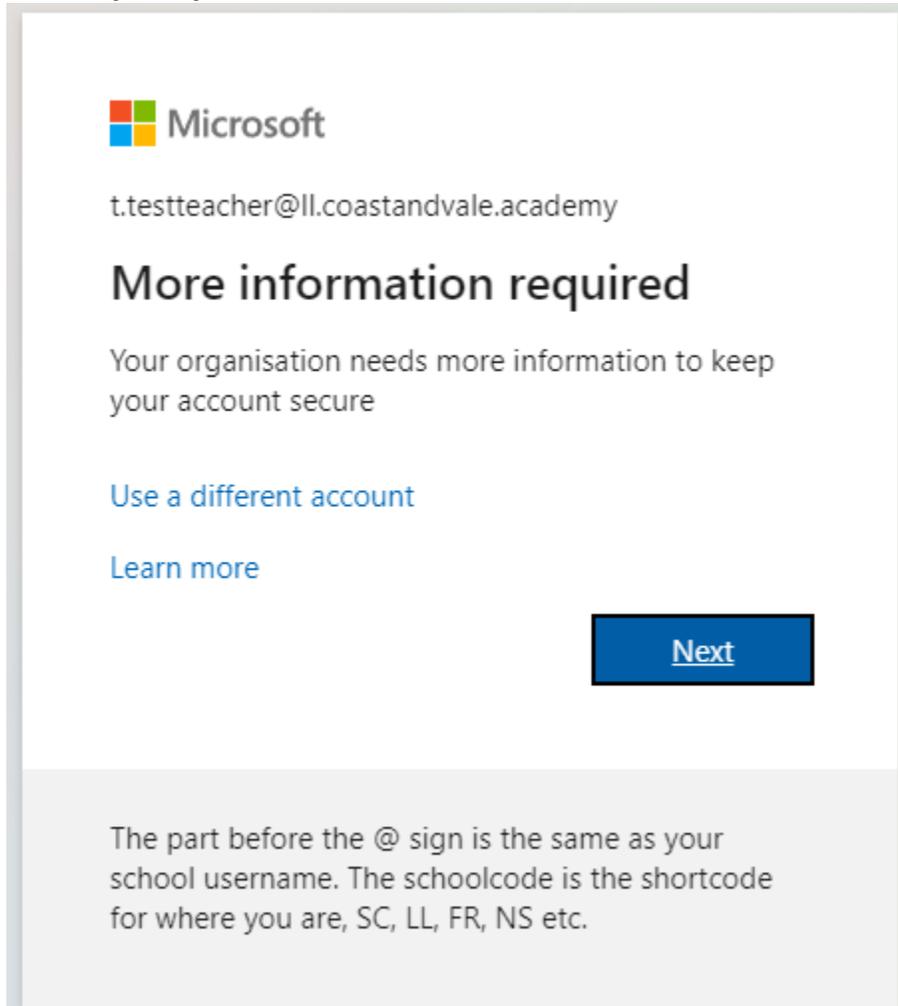
Click the "Next" button to continue.

On the next screen you will be presented with the default, recommended, method which is the Microsoft Authenticator app.

Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Next

I want to set up a different method

ℹ️ If you do not want to use a mobile phone or app, click "I want to set up a different method" (highlighted). This will allow you, at the time of writing, to opt to use a telephone number. This is detailed below as "Method 2".

Method 1: Authenticator App

As the image above, you are instructed to download and install the Microsoft Authenticator app on your device. There is a link to click to be taken to the app download.

ℹ️ We will not cover the specifics of installing apps, as that depends on the manufacturer of the device. Refer to your device's app store.

Once you have downloaded and installed the Microsoft Authenticator app, click "Next" on the screen. You will see this page:

Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back   Next

I want to set up a different method

Once the authenticator app is installed, it will be required to send notifications. Your device may prompt if you wish to allow notifications (as per the image above). If relevant, allow notifications and click "Next".

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 with your account.

After you scan the QR code, choose "Next".

Can't scan image?

Back   Next

I want to set up a different method

Use the Microsoft Authenticator App to scan the QR code. This will bind the authenticator to your account so only you can access your account via the secondary method. The app should successfully detect your account and add it.

You will then be prompted to check it's working. Your device/app will produce a notification you need to approve. Once done, click Next.

If you successfully receive and approve the notification, the web page will automatically update with the approval:

That's it, you're all set! Whenever you sign in off-site, you will need to approve the authentication so that we know it's really you. This will stop anyone else trying to gain unauthorised access to your account as they will physically need access to your mobile device too.

Method 2: Phone

If you don't wish to use the mobile app, click "I want to set up a different method". You will see the following pop-up, drop the list down and choose 'phone', and then confirm the choice

Choose a different method ✕

Which method would you like to use?

Phone ⌄

Cancel   **Confirm**

At the following screen, choose "United Kingdom" from the list of countries, enter your phone number and click Next:

Phone

You can prove who you are by texting a code to your phone.

What phone number would you like to use?

United Kingdom (+44) ⌄   0▮▮▮▮▮▮

⦿ Text me a code

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

Next

The following screen will confirm that Microsoft have sent a message to your phone. You should receive a text with a code, enter the code into the web page and click "Next".

ⓘ If you didn't receive a code, click "resend code".

Phone

We just sent a 6 digit code to +44 0▮▮▮▮▮▮ Enter the code below.

357102

Resend code

Back   **Next**

If the code is correct, the next pages will verify this:

Phone

✅ SMS verified. Your phone was registered successfully.

Next

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

📞 Phone
+44 ████████

Done

You will now be set up to use text-based verification as your two-factor method. Whenever a sign-in attempt is made, you should automatically receive a text.