Setup Multi-factor Authentication on your College Account

What is MFA?
MFA adds additional security to your College account which makes your account almost impossible to hack. It adds a second level of authentication (in addition to your password) to your login process – the second level is normally by entering a code that you receive via an app, text, or voice call.

You simply need a phone that you can use to either install an app onto or to receive text or calls.

Once setup, you will be asked for the second form of authentication whenever you logon to an Office 365 application from outside of the College, or login on to a personal device on-campus. You will not be asked for MFA when you log on to a College-owned device on-campus.

The process currently works for all Office 365 applications (Email, OneDrive, Teams, etc). The College ICT team will add further applications to this service to further protect your data and account.

Once you have setup MFA the process for logging onto a service will be as simple as the following:

1) Go to your URL of the application you want to access.
2) Enter your username & password
3) Provide the second form of authentication via an app, text or voice call to a mobile or landline number.

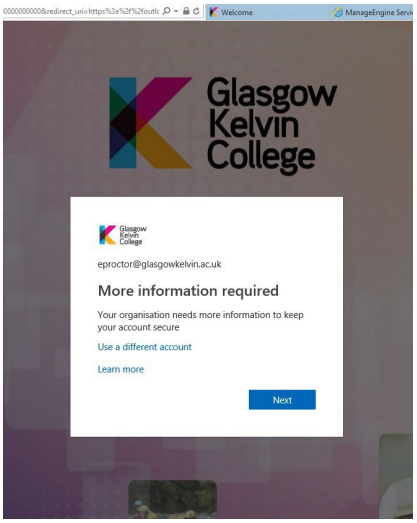
You will be asked to set up MFA the first time you log into your College account. This document will show you:

- How to set up MFA
- How to use MFA when you log in to your Office 365 account

How to set up MFA

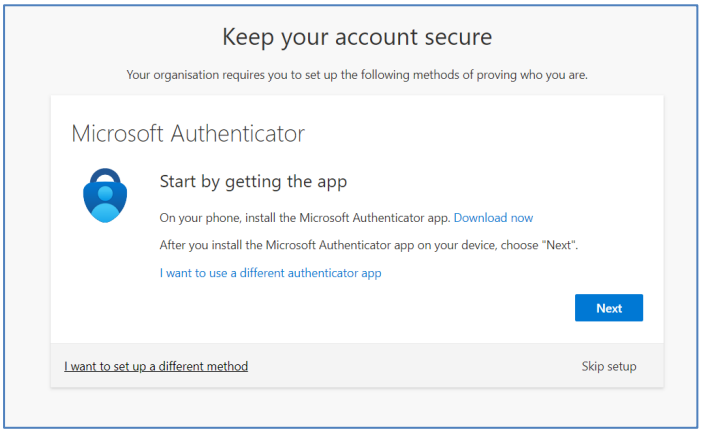
1) Log int to your Office 365 account with your College email address and password by going to https://outlook.com/glasgowkelvin.ac.uk. As this is your first time logging in, you will be presented with the screen below, which is the start of the MFA setup process:

   Click **Next.**



2) At the next screen you will be asked to choose how you should be contacted to authorise MFA. ICT recommend using the Microsoft Mobile App, so this is the default option.

   If you want to receive authentication codes by text or voice call, then go to Appendix A – Use an alternative method for MFA



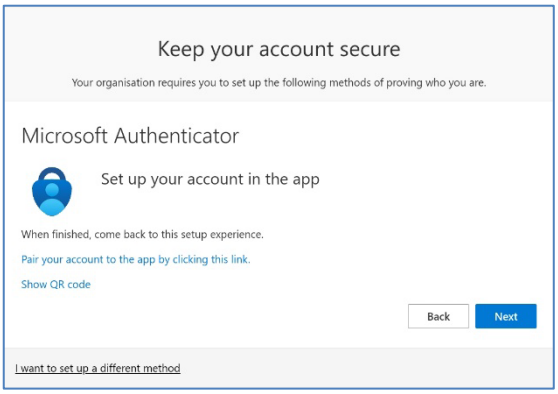
   *From this screen you can click on the **Download now** link that will take you a page that displays QR codes for the Authenticator App in the iOS and Android stores.*

   You can also use the links below:

iOS - https://itunes.apple.com/gb/app/microsoft-authenticator/id983156458?mt=8
Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_GB

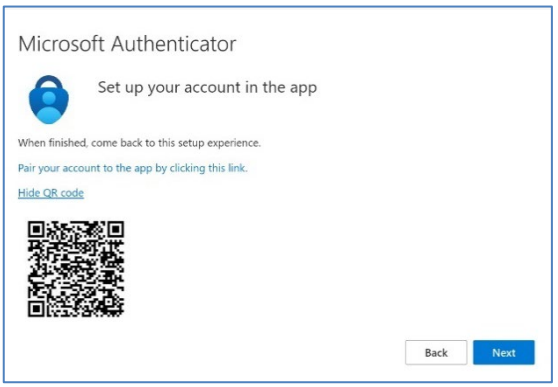
Once you have the app installed, click on **Next.**

3) At the ***Keep your account secure*** screen, click on **Show QR code**.

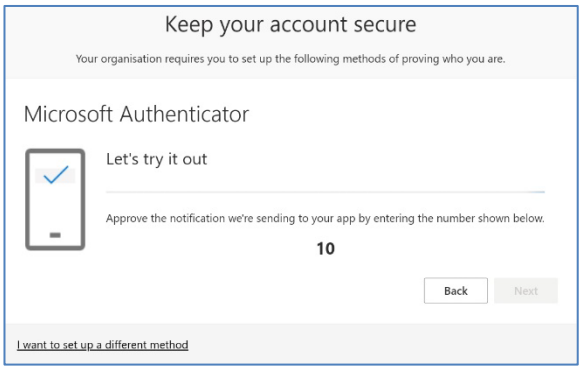


4) Follow the on-screen instructions and scan the QR Code with the Authenticator app.

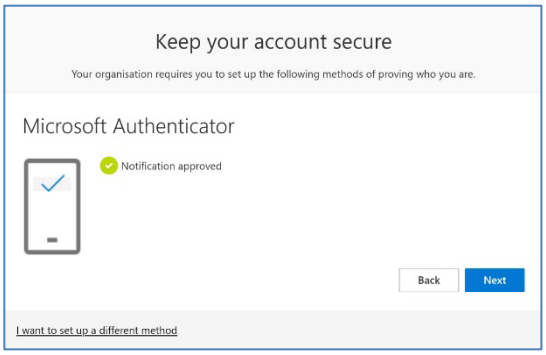
Click **Next**



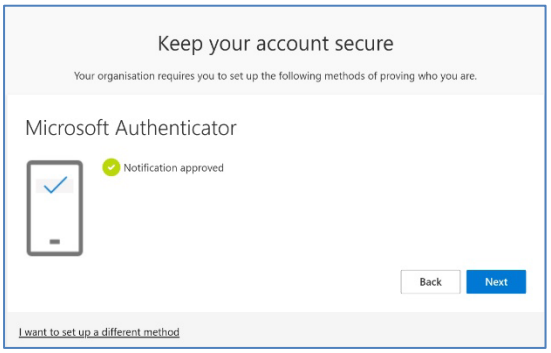
5) On the next screen, enter the code shown on-screen into the Authenticator app to confirm that MFA has been successfully set up.



Once you have entered a valid code you will be able to click the **Next** button



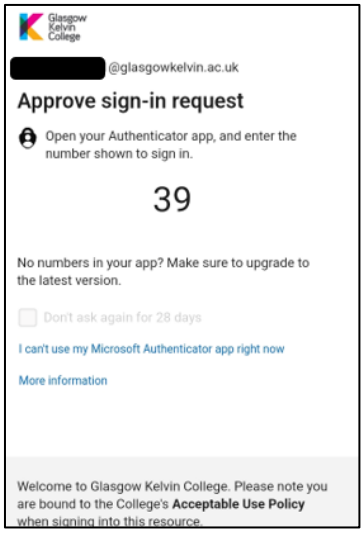
At this point you will have completed the MFA setup and you can click on the **Next** button to exit the MFA setup and log into your Office 365 application.

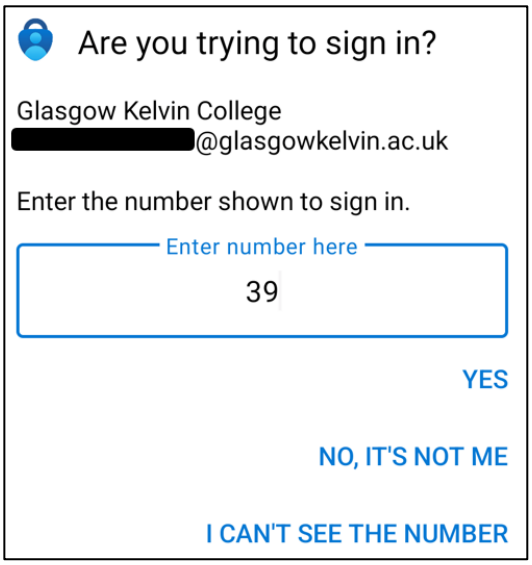


6) Once you have set up MFA, you can select the **Stay signed in?** option so that you won't be asked to authenticate on the same device for 28 days.

   *If you are signing in on a device that is used by other people, we recommend **not** selecting this option to keep your account secure.*

7) From now on, when you log into your Office 365 account, you will be asked to approve the sign-in request on the authenticator app (or to enter a code if you have opted for text or voice call authentication)





Further help & Information

Remember only to approve a MFA request if **you** are trying to access a College service. If you're not trying to access a college system and you receive a request, it may signify that someone is trying to hack your account.

You will only be asked for MFA when you are logging in from outside of the College, on-campus logins will not be affected.

If at any point you want to change your MFA settings, then go to this URL –
https://account.activedirectory.windowsazure.com/proofup.aspx
Or -
https://mysignins.microsoft.com/

You can also access this URL in Office 365 by doing the following:

- Clicking on your account picture in the top right of Office 365
- Clicking **View Account**
- Clicking **Security info**

From here you can add additional authentication methods or change your existing information, such as a mobile phone or landline number for voice calls.

Appendix A – Use a text message to be contacted for MFA

Microsoft strongly recommend using the Authenticator app as it's more secure than the alternative of text or voice call. However, if you can't install the app, then you can use one of these alternative authentication methods. ***Please note that charges may apply for text messages or calls to a mobile or landline number.***

Setting up MFA using text

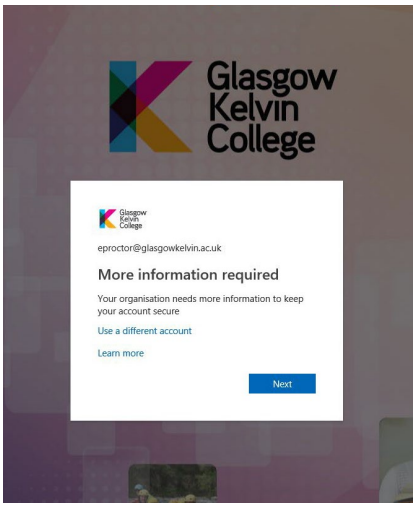
Please note that if you register a mobile phone number to receive MFA codes by text, Microsoft will send the MFA notification to WhatsApp, if you have it installed on your mobile phone. This is because WhatsApp's end-to-end encryption is more secure than text messages.

If you don't have a WhatsApp installed on your phone, or you uninstall WhatsApp from your mobile phone, Microsoft will send the MFA notification by text as normal.

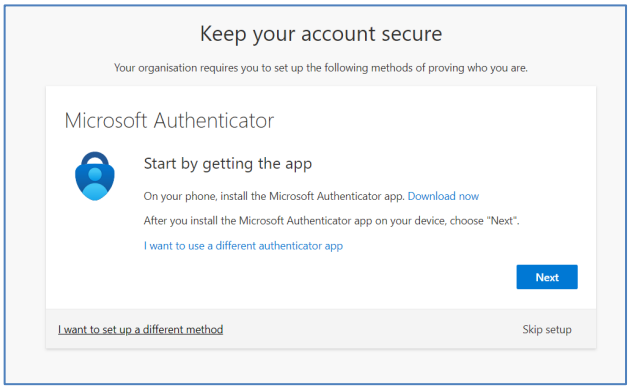
1) Log into your Office 365 account with your College email address and password by going to https://outlook.com/glasgowkelvin.ac.uk.

As this is your first-time logging in, you will be presented with the screen below, which is the start of the MFA setup process:

Click **Next**



2) At the next screen you will be asked to choose how you should be contacted to authorise MFA – the default method is to use the Authenticator App.

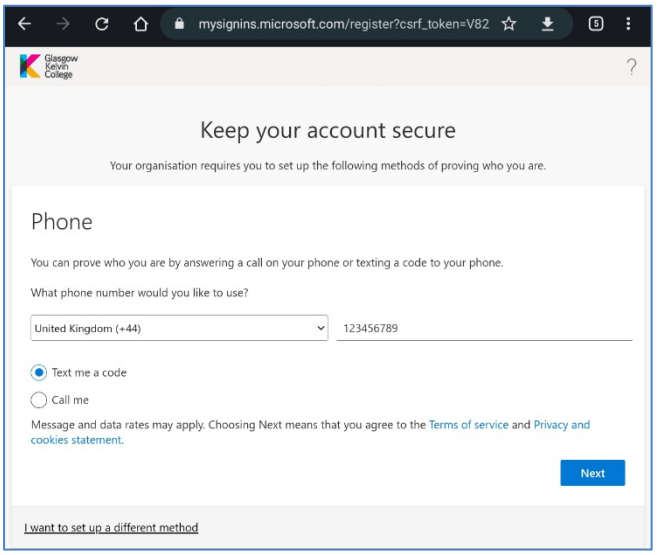


Click on **I want to set up a different Method** and choose **Phone**

3) Select the International Dialling Prefix for your phone provider from the drop-down list.

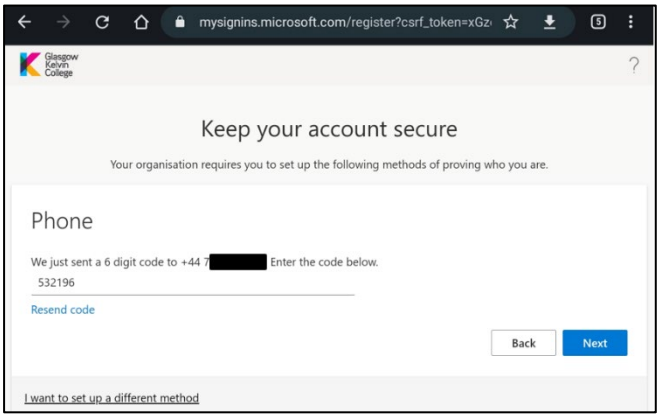
   Then enter your mobile number, or a land-line number (without the leading "0"). If you enter a landline number and your phone provider doesn't offer a text-to-voice service, you can select the **call me** option.

   Then click **Next.**



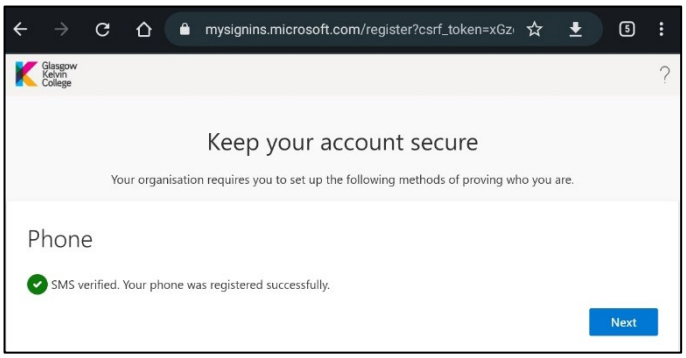
4) Enter the 6-digit code sent to your phone.

   Then click **Next.**



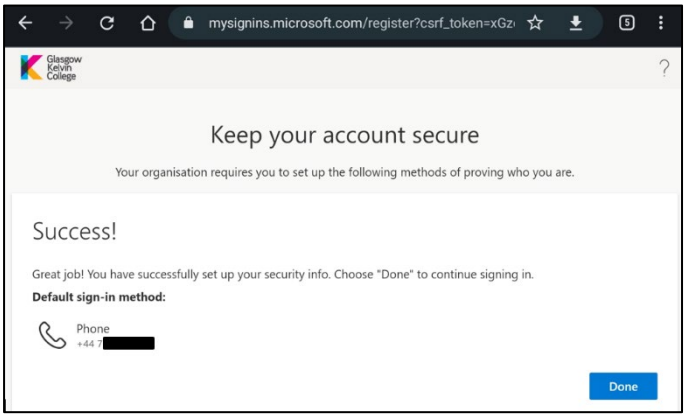
5) If you have entered a valid code, the next screen will confirm that the phone number has been registered for MFA authentication.

   Click on **Next.**



6) Once you click **Done** you will be taken to back to the Office 365 login screen to finish login in by authenticating an MFA request.

   You are now setup with MFA, if you attempt to login from outside of the College you will receive an MFA request.



******* END OF DOCUMENT *******