**How to enable Multi-Factor Authentication (MFA)**

To enhance our security protocols, we are introducing Multi-Factor Authentication (MFA) to provide an extra layer of protection for our systems and data. This will require everyone across Enginuity and EAL to verify their identity through multiple methods, ensuring stronger defence against unauthorised access.

From 21st August, you will be prompted to set up or verify your identity using the MFA security feature when attempting to access any EAL application.

**Important:** If your centre, or anyone at your centre, is unable to use any of the authentication methods outlined in this guidance, please submit a ticket to our Customer Experience team via the chat on EAL Connect. Alternatively, please contact the Customer Experience Team via Customer.Experience@eal.org.uk or 01923 652400. They will assist you with your query.

Subject to approval - where restrictions or unique circumstances prevent the use of the MFA methods listed, users may be eligible to receive their authentication code via SMS or email.

Authenticator applications covered by this guidance

* Google/Microsoft Authenticator verifies your account by generating a single-use code through the mobile app.
* OKTA Verify, verifies your account through a push notification sent directly to your mobile device or by using a single-use code generated by the app.

When setting up your MFA for the first time, please follow these steps:

Step 1:  Attempt to log into any EAL application, such as EAL Connect in this example. Enter your email address and click 'Next':

Step 2: You will be prompted to enter your password. Enter your password and press ‘Verify’:

Step 3: You will now be required to download an Authenticator app from the Apple/Google Play store. You can use either the Google Authenticator or Microsoft Authenticator app. To begin setup, download your chosen app, then click the ‘Set Up’ button under the Google Authenticator section on the screen:

Step 4: Open your Google Authenticator app, click the plus button in the bottom right corner of the screen and select ‘Scan a QR code’ (highlighted in red): 

Using your phone camera, scan the QR code displayed on your laptop screen and press ‘Next’:

Alternatively, if you are already using the OKTA Verify application, select ‘Set up’ button under the Okta Verify section:

For OKTA Verify, you will need to select your device type, either iPhone or Android, and then click ‘Next’:

Once you have the OKTA Verify app ready, scan the onscreen QR code and follow the in-app instructions to complete the setup process.

If you need any further support, please contact the Customer Experience team.