

## Non-CAC Secure Access with Multi-Factor Authentication (MFA)

### Anytime, Anywhere - Securely

For years, DoDEA has required the use of a your common access card (CAC) and pin to verify staff identity. Imagine being able to be mobile and having the flexibility to access resources whenever you need them - even if you do not have your CAC.

To maximize access to DoDEA online resources while continuing to protect access to DoD systems and data, staff will be able to setup non-CAC secure access using multi-factor authentication (MFA) through [Microsoft 365](#). MFA validates who you are in multiple ways using passcodes, phone, email and/or other unique factors. This option allows you to **access more DoDEA resources anytime and anywhere**. \*Most DoD systems will continue to require a CAC and pin.



### How Multi-Factor Authentication (MFA) Works

Multi-factor authentication requires that you verify your identity in **at least** two different ways:

- **Something you know** – such as your username and password, a secret code or answers to private questions
- **Something you have access to** – such as an access card, phone, email
- **Something you are** – such as your fingerprint or iris scan, or DNA

For DoDEA purposes, you will use:

- **Something you know** (username and password), **PLUS:**
- **Something you have access to:** your office phone, mobile phone or mobile app for Android or iPhone.