Set your Microsoft MFA options
Download Microsoft Authenticator App for your mobile phone
Download Microsoft Outlook App for your mobile phone
Set up your 2 Step Verification for Google

What is Multi-factor Authentication (MFA)?
Multi-factor authentication (MFA) decreases the likelihood that others can access your data. It enhances the security of your ID by using your phone, tablet, or other device to verify your identity when you attempt to access your accounts. You may have already seen MFA on your banking accounts, social media accounts, and other online services.

MFA takes two verifiable items to allow access to your information: "something you know" (like your password) and "something you have" (like your phone). For example, when you visit an ATM, one authentication factor is the ATM card you use to start the transaction - that's the "something you have." Next, you enter a PIN, which is the "something you know." Without both factors, you cannot access the account. MFA is a simple way to keep bad actors out of your account. It also provides the same benefit to FCPS, protecting important information like student data, HR records, and personal information about you.

What are some applications and systems in FCPS that are protected with MFA?
- VPN
- FCPS Google applications and data
- FCPS Microsoft Office applications and data
- FCPS Employee Hub
- Zoom

Are these the only applications and systems in FCPS protected by MFA?
As we refine our security settings over the next year, we will be bringing a number of applications and systems under MFA protection.

How do I set up MFA?
The simplest way is to use an Authenticator App on your phone. Once that is set-up, and you attempt to log into an MFA protected account, the application will send an instant notification to the authentication app on your phone to ask if you approve the log-in. This method is an extremely quick way to authenticate via MFA. Though slightly less efficient, other methods are also available. Please speak with your TSSpec about those options.

What if I don't have an FCPS phone?
You can set up an authenticator app on your personal smartphone. It does not have to be an FCPS phone.

If I use my personal phone to authenticate, doesn't that make it susceptible to FOIA?
No. An authenticator app does not store any documents or data that would be applicable to a FOIA.

- **Will I be prompted every time I access one of the applications listed above?** Not on an FCPS-issued laptop. We have worked to strike a balance that protects FCPS systems, while minimizing disruption to your work. If you use the same FCPS-issued laptop every day, you will find that when you provide MFA for one application (i.e. VPN), in many cases it will remember that authentication in other places (i.e. Microsoft Office).
- Other devices, including non-FCPS devices, may or may not remember a previous response. These factors vary by device, application, and the settings on that device.

Will I be prompted once for each application?

- Not on an FCPS-issued laptop. We have worked to strike a balance that protects FCPS systems, while minimizing disruption to your work. If you use the same FCPS-issued laptop every day, you will find that when you provide MFA for one application (i.e. VPN), in many cases it will remember that authentication in other places (i.e. Microsoft Office).
- Other devices may or may not remember a previous response and depends on the device, application, and the settings on that device.

I am prompted for MFA access on some devices or applications more than others.

The security requirements can vary by the level of risk presented by the application and/or data. If the data you are accessing is highly sensitive, you will likely be prompted for MFA more frequently in that application or system.