# MULTI-FACTOR AUTHENTICATION (MFA)

## BACKGROUND

All staff accessing District information are responsible for the management and protection of sensitive information under their control to prevent unauthorized access and ensuring compliance with privacy and security legislation. This requires the use of Multi-Factor Authentication (MFA) which adds security to prevent unauthorized access to systems, applications, and data on supported platforms.

### Definitions

- **Multi-Factor Authentication (MFA):** A security method that requires users to provide two or more verification factors to gain access to a resource.
- **Primary Credentials:** Usually, a username and password.
- **Secondary Factors:** May include a mobile app (e.g., Microsoft Authenticator), SMS code, or hardware token.

## 1. Scope

1.1 This procedure applies to:

a. All employees, contractors, augmented staff and third-party users that access network or data resources managed by the school district.
b. All systems and applications transmit sensitive or confidential information.
c. Remote access to internal systems and cloud-based services.

1.2 All users must use MFA when accessing:

a. Productivity suites like Microsoft Office 365 and related platforms
b. VPN or remote access solutions.
c. Cloud platforms that support MFA mechanisms
d. Administrative interfaces and privileged accounts.
e. Any system containing sensitive or regulated data.

1.3 Use of MFA is mandatory, as not enrolling in MFA will restrict access to district provided application and service platforms. Exceptions to this policy must be approved by the IT Security Team and documented with a valid business justification.

## 2. Enrolment

2.1 MFA must include at least two of the following:

a. Primary Credential
b. Secondary Credential

2.2 As a Secondary Credential, authenticator apps, SMS-based MFA or a District-provided hardware token will be provided.

2.3 For staff members with no cell phone (District or personal), or do not which to use their personal device, the District will provide hardware tokens. The care and proper use of these tokens will be the staff member's responsibility.

2.4 Staff members with no cell phone, or do not wish to use their personal cell phone, must use District provided hardware tokens. Care and proper use of these tokens will be the staff member's responsibility. Lost fobs will be replaced for a cost to the employee.

2.5 Staff using personal devices for MFA must ensure they are secured with passcodes and updated regularly.

2.6 The district does not assume responsibility for costs associated with personal device usage unless previously approved.

## 3. Non-Compliance

3.1 Failure to comply with MFA requirements may result in suspension of access to district systems.

***References:***
***Adopted: October 09, 2025***
***Revised:***