# Multi-Factor Authentication

## | Document Information |

Category: Guidance |  
Created: 2022-03-04 |  
Domain: Sector Security |  
Author: pete.dingwall@education.gov.uk |  
References: GUI-SEC001 - MFA Guidance |

## Introduction and Background

The Department has seen a number of cyber incidents which have been the result of weak controls for accounts which can grant a malicious user access to a school’s systems. Cyber criminals are adept at carrying out brute-force attacks on systems which are exposed to the Internet and which could provide access, and will use common passwords and variations, and will also check password lists from systems which have been previously compromised such as LinkedIn, Adobe and others.

The use of Multi-Factor Authentication (MFA) will immediately stop this, as it is no longer sufficient to simply provide a username and password. In order to access the system the user needs to provide **something they know** (username and password) and **something they have** (a one-time passcode, an approval from an app, a hard token etc).

Any attempt to guess a user’s password to access a system is therefore no longer possible, as the additional factor is also required and will not be available to the malicious user.

### Further benefits of MFA

The use of MFA also ensures that users are not sharing accounts as only the person with the additional authentication factor is able to access the system. MFA also stops accounts being handed over to users if they change roles or leave an organisation, as the person taking on the acount will not have the additional factor and will therefore not be able to access the account.

MFA can also be used for what is known as *risk-based authentication* where a user may be accessing a system when there is heightened security due to a malicious attempt to access, or where other areas of a school’s systems have been accessed. It could simply be the case of a user accessing outside of their normal hours, or during a holiday, or from an unfamiliar location. MFA can also be used in these circumstances as extra proof of a person’s identity to verify and assure that their account is not being used maliciously.

## Principles for the use of MFA

Whilst MFA is a useful security control, it can also be seen by users as adding additional burden to their daily routine. It is important therefore that it is used appropriately to ensure that end-users are not unnecessarily inconvenienced, and also to ensure that it is not circumvented due to being difficult to use.

### 1 - Review existing guidance

*Existing guidance can be used for broad best practices and principles*

#### Why?

The National Cyber Security Centre (NCSC) provide general broad guidance which is suitable for all institutions seeking to find out more about MFA.

#### How?

* Review the guidance found at https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

### 2 - Apply MFA proportionately

*MFA should only be used where required, and does not have to be for all accounts*

#### Why?

MFA is used to protect access to accounts and systems which could be used maliciously to gain access to systems and data, remote access to a schools systems or to enable malware to be deployed to a school.

MFA is generally charged on a per-user basis, and could therefore be expensive to deploy to all users within a school, and the impact of applying MFA for all school users could be disruptive for both the implementation and management of the system.

#### How?

* Good security is achieved with a number of controls, with MFA being part of this solution in conjunction with best practices to manage access to critical systems and data
* Apply MFA to the relevant roles only. A read-only account may not require MFA if it does not expose any critical data, but an account which can be used to change critical systems should be protected
* Consider the impact of an account being compromised when considering the need for MFA. A student account being compromised would enable access to the student’s work but would not cause significant widescale impact to the school, therefore MFA woud not be appropriate for students
* Costs for MFA will rise if applied to all users, and this may be a barrier for not using MFA. The Department would rather see a smaller deployment of MFA for critical systems and users rather than not at all

### 3 - Identify systems which cannot support MFA

*Systems which cannot support MFA will pose a risk of compromise*

#### Why?

Some systems and services used by a school may be perfectly adequate for providing their core service, but unable to support the use of MFA due to their age, or lack of support from the vendor. The lack of MFA support due to age or lack of support may highlight other potential vulnerabilities, so these systems must be identified and tracked,

#### How

* Wherever possible, plan to upgrade the service so it can support MFA
* If the service cannot be upgraded to support MFA, or this is not available, seek to replace the service so it can be secured appropriately
* Ensure that any system which cannot suport MFA is captured in your risk logs
* Take steps to secure the system by strengthening passwords, reducing access and ensuring the any users who have access are regularly assessed
* Where possible, monitor access to the system to identify any inappropriate access
* Seek to apply network separation if available to ensure that any malicious access to the system cannot be used to gain access to the wider school network

### 4 - Use MFA to protect critical systems and accounts

*MFA should be used appropriately to protect systems which could be used maliciously*

#### Why

Certain systems and system roles are attractive to malicious users as they can be used to gain access to a school’s systems, and can provide super-user access to enable access to other systems and data. MFA can be used to protect access to these systems to ensure that they are only accessed by authorised personnel.

#### How

* Identify your critical systems and apply MFA to any accounts which provide administrative levels of access. Examples of systems which should be protected are:

1. Active Directory
2. Cloud platforms (Google Workspace, Microsoft 365)
3. Web hosting platforms (sites used to host school websites etc)
4. Financial systems (accounts, MIS etc)

* As outlined in **Principle 1**, ensure that MFA is only used where required. Consider the end-user impact and ensure that MFA is only applied to system roles which could be used for malicious access or to gain access to valuable data
* Adhere to **Principle 2** for any systems which cannot support MFA

### 5 - Use MFA to protect specific school roles

*MFA should be used to protect high-profile and senior roles*

#### Why

Cyber criminals will seek to target specific users in schools who hold key roles which would be useful to gain access to specific data or systems. Criminals will also target specific users to spoof their identity for social engineering attacks, where a user may be more willing to click on a link or provide information if the request is from a senior person within a school

#### How

* Identify your key roles and users, and apply MFA to any accounts. Examples of roles and users which should be protected are:

1. Senior Leaders within a school
2. School Governors
3. Teachers with access to critical systems or data

### 6 - Ensure MFA is used on any remote access systems

*Remote Access systems are targeted by malicious users and must be protected*

#### Why?

Remote access systems are easy to identify s as they tend to give away their presence with common signals which malicious users can look for on the Internet. Once they have gained access to a school’s remote access system they can then use that to access other key systems, deploy malware and steal data.

#### How?

* Ensure that MFA is applied to any user who has access to remote access solutions. Some examples of these are provided below:

1. Any remote desktop systems (Remote Desktop, RemotePC, ZoHo etc)
2. Any Virtual Private Network (VPN) solutions (Cisco Anyconnect, F5 Access etc)

* Adhere to **Principle 2** for any systems which cannot support MFA

### 7 - Protect facilities systems

*Systems used to manage facilities are targeted and can also be used to gain physical access*

#### Why?

A school will often have separate facilities used to manage “CCTV” cameras, physical security for the site and *Building Management Systems* which control heating and air-conditioning for the school. These systems are often connected to the main IT network in the school and can therefore grant access to other systems if a compromised.

#### How?

* Review all systems which manage a school’s facilities systems and review whether they can support MFA
* Apply MFA to the relevant accounts for each system to protect from malicious access and use
* As outlined in **Principle 1**, ensure that MFA is only used where required. Consider the end-user impact and ensure that MFA is only applied to system roles which could be used for malicious access or to gain access to valuable data
* Adhere to **Principle 2** for any systems which cannot support MFA

### 8 - Use well known MFA providers and standards

*Well-known providers of MFA services are likely to provide good support and be compatible with most systems*

#### Why?

The MFA market is crowded with numerous suppliers offering similar services for different prices. Cheaper options can often seem attractive but may not offer adequate support or compatibility.

#### How

* Review existing technology providers in-use and review any MFA solutions they provide
* Prefer provides who supply MFA solutions *as-a-service* from a cloud platform, as this will be supported, patched and maintained on your behalf
* Seek suppliers who support authentication standards such as FIDO2, as these are recognised standards and will be compatible with most modern systems

### 9 - Use appropriate types of MFA

*Review the users of MFA services and utilise the most appropriate type of factor*

#### Why?

Multiple MFA factors are available for end-users, and a well-researched and selected product, which is appropriate for your users’ needs will help to ensure a successful use of MFA.

Examples of factor types are: 1. Physical tokens, which are inserted to a USB port in a computer 2. SmartPhone Applications which provide a signal/prompt to verify an authentication attempt 3. One-Time-Passcodes (OTPS), which are random 6-8 figure numbers which are generated on a 60-second cycle by a physical token or an application

#### How?

* Review the users who will use the MFA solution
* Review their location requirements - will access to a phone be possible?
* Review the management of tokens - if the users are remote how will you send out and manage physical tokens
* Review their physical requirements - will users be able to utilise a OTP solution, if they are not familiar with SmartPhone apps
* Review the IT maturity of the users - a simple physical token may be the most simple solution for less IT-confident users