**Contents**

[**1.** **Identity and access management** 3](#_Toc83217235)

[**2.** **User authentication** 3](#_Toc83217236)

[**3.** **How authentication works** 4](#_Toc83217237)

[**4.** **User authentication methods** 4](#_Toc83217238)

[**Passwords** 4](#_Toc83217239)

[**Biometrics** 5](#_Toc83217240)

[**Email Authentication** 5](#_Toc83217241)

[**5.** **How to improve user authentication** 5](#_Toc83217242)

[**Multi-Factor Authentication** 6](#_Toc83217243)

[**Policy Requirements** 6](#_Toc83217244)

# **Identity and access management**

Identity and access management refers to the collection of policies, processes, and systems which identify and control permissions for performing functions and accessing information.

If identity and access management procedures and controls are badly designed or implemented, they can give attackers an easy way to gain access to your systems.

There are several areas of identity and access management:

* **User authentication and authorisation covering** how you establish the identity of a person and check permissions.
* **System architecture -** secure design of the computer systems that support the above areas. NCSC's [Design Principles](https://www.ncsc.gov.uk/collection/security-design-principles-digital-services-main) may be useful.
* **Operations and monitoring -** the supporting processes and technology to identify and enable investigation of breaches of policy or controls.
* **Policy which governs** who is authorised to access systems, data, or functionality, how they can request access, when their access should be removed, how issues are reported, and what the expectations are for security.
* **Privileged user management -** the additional processes and controls you should put in place to safeguard the most privileged (admin) accounts. This is covered in a separate guide.

# **User authentication**

User authentication is the process of proving that a user is who they claim to be and have approval to access the systems they are attempting to logon to. User **authentication asks** each user, “Who are you?” and uses the response they provide to check their right of access.

When a user has an account for a system / app, they are given, or they create, a **unique identifier (ID)** and **key** that will allow them to access their account later on.

In most cases, in school, the **ID is the username** and the **password is the key**, but the credentials can include other forms of keys as well.

User authentication is the process used to validate legitimate access requests, while attempting to block any *unauthenticated*users from gaining access.

# **How authentication works**

In order to gain access to school systems, users must prove they are who they say they are, by providing their ID and key. If they provide the correct credentials, the user is authenticated. This is NOT the same as authorisation.

Authorisation and authentication are often used interchangeably, the two terms are different. BOTH are needed to secure user access.

**User authentication** verifies users’ identities and approves or declines access. **(Who)**

**User authorisation** verifies the type and level of access – known as permissions. **(What)**

When a match is found, the system will authenticate users and grant them access to their accounts. If a match isn’t found, users will be prompted to re-enter their credentials and try again. After several unsuccessful attempts, the account may be flagged for suspicious activity or require alternative authentication methods such as a password reset or a onetime password.

# **User authentication methods**

In order for a user to confirm their identity, the individual must provide a piece of information that only the user and the server knows.

This information is called an authentication factor, and there are three types:

|  |  |  |
| --- | --- | --- |
| **Knowledge factors** | Factors the user must **know** | Username / password / PIN |
| **Possession factors** | Anything the user must **have** | Key fobs / ID Cards / SMS message |
| **Inheritance factors** | Using a person’s **biological characteristics** | Fingerprint / voice / facial recognition |

# **Passwords**

Most users are familiar with passwords. In fact, passwords have been the tried-and-true method for user authentication since the beginning of the internet.

Passwords are often used to secure accounts, but they are *not*as secure an option as many users think they are. Users should never share passwords and passwords should be a **minimum** of 8 characters. The NCSC has updated [password guidance](https://www.ncsc.gov.uk/collection/passwords/updating-your-approach).

Many users use the same password for every system. This can lead to ‘credential (password) stuffing’ where criminals use stolen credentials from one system to attempt access to other systems, acting on the assumption that the passwords will be the same.

# **Biometrics**

This type of user authentication is often considered one of the most secure options for users because everyone’s biological characteristics are unique and can’t be easily duplicated. It also means that end-users can’t lose access by misplacing fobs and ID cards.

Fingerprint scanning is increasingly being used in schools. Schools must be sure that they implement such systems with regard to Data Protection Act 2018 legislation. Biometric data is special category data under the act and requires a valid legal basis for processing.

See the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4) for more information.

# **Email Authentication**

The email authentication process can look different depending on **technical solution chosen. It aims to prove that an email is not forged and** comes from who it claims to be from.

Email authentication is most often used to block harmful or fraudulent uses of email such as phishing and spam.

# **How to improve user authentication**

Stronger user authentication keeps unauthorised users from gaining access. Authorisation ensures that sensitive information is protected from users who do not need access.

When your user authentication isn’t secure, however, cybercriminals can hack the system and gain access, taking whatever information the user is authorised to access.

Improve your user authentication:

* Enforce the minimum requirements through **school policy.**
* Enable **Multi-Factor Authentication** (MFA)
* Longer passwordsare more secure and although a **minimum of 8 characters** is suggested, it is recommended that passwords are closer to 12 characters in length.
* Passwords should have a **mix of characters**, uppercase and lowercase letters, numbers, and symbols make it harder to crack.
* Use a **different password for each account** and, if you can’t remember numerous passwords, use a [Password Manager](https://www.ncsc.gov.uk/cyberaware/home#section_3).
* **Make your password random** and don’t use dictionary words or personal information.

# **Multi-Factor Authentication**

Multi-factor authentication (MFA) can also be called two-step verification or 2-factor authentication (2FA). The [2FA Directory](https://2fa.directory/) has a list of websites and whether or not or not they support 2FA. The [NCSC has guidance](https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services) on this.

# **Policy Requirements**

An identity and access management policy would typically cover:

* Who should have access to certain systems, data, or functionality and why.
* The circumstances under which access is granted or revoked (removed). This requires a robust starter/leaver process – see our additional guide.
* An analysis of which actions or processes, if any, should require multiple people to perform them. (Data maps and information audits, required for data protection compliance, will support this.)
* Actions which should be monitored, recorded, how audit records are acquired and how they are safeguarded against tampering.
* A documented Privileged User Policy should cover the process of authorising admin accounts.