Authentication/Access Policy Guide and Template

Authentication is a process to ensure that only users with the correct login/access details are allowed to access digital and online schools resources and systems.

The use of usernames and passwords is still the most conventional method of authentication/access used by schools, and though there are some alternative approaches available, we'll focus on this method here.

General Guidance

- Users passwords must be treated confidentially, and not disclosed to any other internal or external school parties. If passwords are disclosed, lost or compromised another party could use these passwords to gain unauthorised access to school systems, and this could result in a cyberattack, loss or theft of important school data, or a schools data breach.
- Usernames associated with a school should only be disclosed publicly where it is necessary to do so, for example a school contact email address on a school website.
- One way to reduce the risk of a school email address being directly copied from a school website by a 'bot' is to change the display format by replacing the '@' symbol with 'at', for example 'info [at] schoolwebsiteaddress.ie'

Guidance regarding Passwords

In a school setting staff and student/pupil accounts are generally set up by a staff member acting in the role of a school system administrator. They assign usernames and temporary passwords to users, on the basis that they change their password after their first login. Users then login using their temporary passwords and change their password to their own confidential password. In primary schools a simpler system may apply, especially for younger pupils.

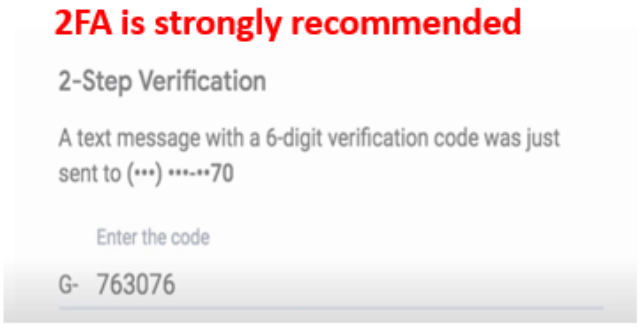
Certain password attributes can be enforced by the administrator, such as password length, use of characters and numbers, lower and upper case letters, special characters etc. However users generally still have a lot of choice and flexibility in creating their own confidential password. Recommended guidance for system administrators should include the following:

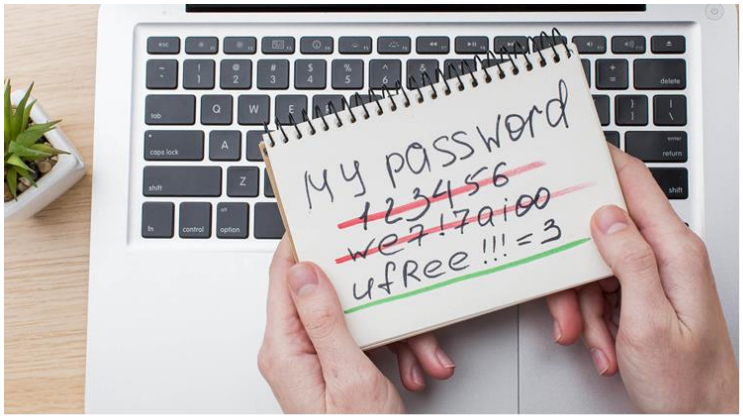
Recommended Guidance on Passwords

- Strong passwords are critical to having a good cybersecurity policy in schools, as this affects all login based access to online activities.
- Good password management can take additional pre-planning, but not doing so exposes the school staff and students/pupils to an increased risk of cyberattack or a data breach.
- Never reveal your passwords to others
- Never use personal/social media login details (usernames or passwords) for work accounts
- To protect user accounts use unique passwords for each different account.
- Never use short passwords as they are extremely easy for cyber-attackers to guess
- Ideally use a minimum or 8 or ideally 12 characters
- Don't just use 'one word' passwords
- Don't use your date of birth, favourite teams, child or pet names, or other words that are easily associated with you, as these passwords can be easily discovered on an individual users social media accounts, in public posts, personal blogs etc.,
- Use passwords that are 'hard to guess' for others, including people that know you, but also use passwords that are relatively 'easy to remember' for you.

- When deciding on passwords use ‘complexity’: eg., include a combination upper and lower case letters, numbers, and special characters as they are much mor difficult for cyber-attackers to ‘crack’.
- One good approach is to use three or four word combination passwords, where the word

https://www.malwarebytes.com/blog/news/2018/09/two-factor-authentication-2fa-secure-seems





https://www.iteksolutions.ca/strong-passwords-the-importance-in-the-workplace-and-how-to-create-one/

- Use Two Factor Authentication (2FA), which uses a combination of two separate ways to login, for example, initially via a password, followed by a short code received on the users mobile phone.
- Remember – a password breach, where your password may be disclosed to other or be made public, doesn’t just affect you. It could also affect your school and work colleagues.
- A data breach or cyberattack could be traced back to a individual user or to a particular device, so all school users need to be aware of and take the necessary steps to help keep the whole school community safe from cyberattacks or a data breach.

Consider using a Password Manager
A password manager is a software application that securely stores and organizes your passwords in a vault. That means you don't have to rely on your memory or on insecure, inconvenient methods like pen and paper. Your password manager does it for you, keeping all your logins securely in one place using high-quality encryption.

Password managers offer a number of advantages in managing users passwords, but before using them users need to understand how they work. High quality password managers are generally not free, though they may offer a limited feature version for free. **One critical fact in using a password manager is that the user is required to remember one 'master' password for the password manager itself.** This 'master' password is only known to the user, so if the user cannot remember it they could lose access to all their passwords and data controlled by the password manager.

However there are many advantages in that users no longer have to remember large number of account passwords.

Essential password manager features:
These include strong encryption, a secure vault for storage, a password generator, multi-device syncing, autofill capabilities, and multi-factor authentication. Other important features are password sharing, dark web monitoring, and the ability to manage the password lifecycle.

- **Strong Encryption:** A password manager should use robust encryption methods like AES-256 to protect stored passwords and other sensitive data from unauthorized access.

- **Secure Vault:** This refers to a centralized and encrypted storage space within the password manager where all credentials and other sensitive information are securely stored.

- **Password Generator:** This feature automatically creates strong, unique passwords for different accounts, reducing the risk of password reuse and weak passwords.

- **Multi-Device Syncing:** This allows users to access their passwords and other stored data seamlessly across multiple devices, such as desktops, laptops, and mobile phones.

- **Multi-Factor Authentication (MFA):** Adding an extra layer of security beyond the master password, MFA requires users to provide an additional verification method (like a code from an authenticator app) to access their vault.

- **Dark Web Monitoring:** Some password managers offer the ability to monitor the dark web for compromised credentials, alerting users if their information has been exposed.

- **Password Lifecycle Management:** This involves features that help manage the entire lifecycle of passwords, including creation, storage, and revocation when no longer needed.

- **Master Password:** A single password that acts as the key to unlock the password manager's vault. It must be strong and securely stored to protect all other passwords.

Some examples of Password Managers

1. RoboForm
2. Keeper
3. 1Password
4. NordPass
5. Total Password

Proposed Authentication/Access Policy 'Template':

The following is the proposed Authentication/Access Policy template that could be used by schools, and inserted as part of their overall school cybersecurity policy.

- The school has a policy in place to control authentication/login to resources for staff, students/pupils and other relevant parties.
- Relevant school staff are provided with authenticated access to relevant school systems, including school staff WiFi, the school learning management system (LMS), the school administration system, and other relevant systems.
- Students/pupils are provided with authenticated access to relevant school systems, including school student WiFi, the school learning management system (LMS) and other relevant systems.
- In order to protect important and sensitive data 'Two-Factor Authentication' (2FA) is mandatory for the school leadership team, the school cybersecurity team, system administrators and school staff for systems including the school learning management system (LMS), the school administration system, and other school systems in order to protect important and sensitive data.
- The school Authentication/Access policy specifies how passwords are managed and controlled. In finalising our policy we reviewed Oide TiE's School 'Authentication/Access Policy Guide' and template which includes guidance and recommended good practice for schools. This is available at https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/ .

If the School Cybersecurity team have any related questions on this area they can email Oide Technology in Education at ictadvice@oide.ie