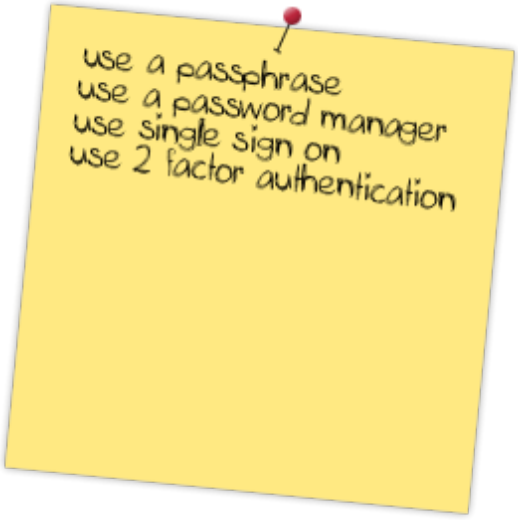
Connected Learning Advisory
Te Ara Whītiki

Recommendations for managing passwords



Password security for schools is a challenging issue. This is because there is a need for a suitable balance between security - protection of information - and usability, or ready access to this information. Poor password practices are a common cause of information being accessed by the wrong people enabling possible harm to individuals. This is why password management requires careful consideration.

This guide covers questions such as:

- Why do I need an online password?
- How often should passwords be changed?
- How complex do passwords need to be?
- How long do passwords need to be?
- Can I ever share my password?
- How do I manage multiple passwords?

This guidance is intended for school leaders and their support staff. The principles are transferable across all consumers of technology.

Contents

Once you have read this guide we encourage you to contact the Connected Learning Advisory for additional personal assistance. We aim to provide consistent, unbiased advice and are free of charge to all state and state-integrated New Zealand schools and kura. Our advisors can help with all aspects outlined in this guide as well as provide peer review of the decisions you reach before you take your next steps.
For more information visit www.connectedlearning.org.nz
Check out our resources at resources.connectedlearning.org.nz
Call us for personalised service on 0800 700 400
Make a personal inquiry via our online form at query.connectedlearning.org.nz
Email info@connectedlearning.org.nz

Summary of Recommendations

We recommend that your strategy for password security should be centred around both highly secure and user-friendly practices. This will increase security with little impact on staff.

We recommend that you use the following – in order of priority:

1. **long phrases** as a password (i.e. a 'passphrase')
2. a **password manager**
3. **single sign on** for those services that allow it, and
4. **2 factor authentication** where possible

Each of these four strategies are outlined below.

We recommend that you **avoid the following**:

- Enforcing regular password changes - only require passwords to be changed if there has been a trigger to require this
- Enforcing overly complex passwords - use phrases instead

Paradoxically, forcing users to change passwords too frequently or have extremely complex passwords can backfire and lead to problems such as writing the password down. The goal is to find the right balance for the different circumstances in your school.

Developing a strategy for password security

There is a wide range of information, data and services in both local and online locations that schools need to protect using a password.

What are you trying to protect?

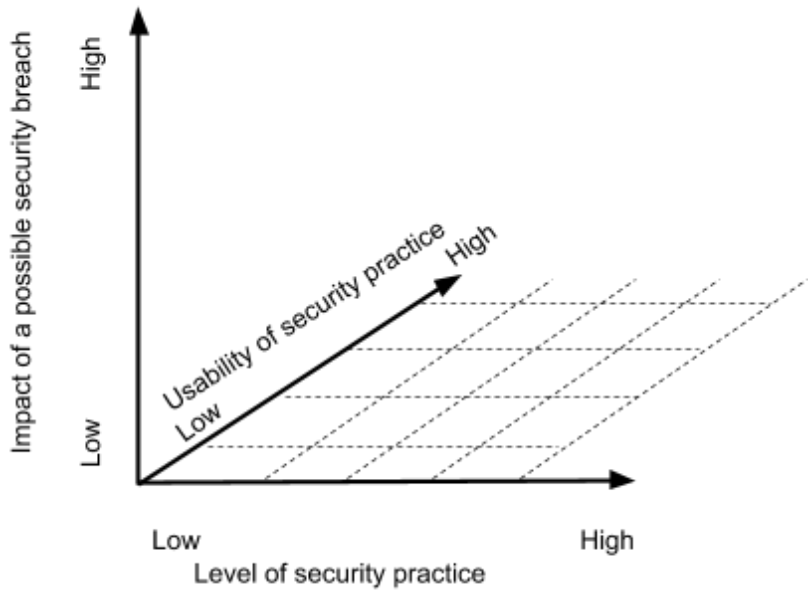
A first step to determining a password strategy for a particular situation is to assess how sensitive the data is and what the consequence would be if unauthorised access were to take place. For example, the more sensitive the information, e.g. personal details about students – including health and behavioural information – the more deliberate the approach should be to security. The safety and security of your students and staff must be paramount considerations.

Evaluate your security practices

The suitability of any password security practice should be evaluated against three criteria:

1. The level of security the practice offers against various forms of attack
2. The degree of security it offers compared to the impact of any potential security breach

3. How useable the security measure is for the staff who will be required to implement it.



Security practices that are both highly secure and readily usable should be encouraged, especially if the impact of a possible information loss (security breach) is also high. If the impact of a possible security breach is low then the level of security can be similarly low.

If the impact of a possible security breach is high and the level of security is low then you have an imbalance and a major concern!

Overall, if we assume that increasing the level of security involves decreasing usability, then the security measures used should be proportional to the impact of a security breach.

For example, the data held in an online platform for creating presentations is likely to be far less sensitive than the data held in your SMS so greater importance should be placed on ensuring the security practices for your SMS. Similarly, measures to secure access to G Suite or Office 365 should be high. This is because these allow staff to not only send school email, but to access previous emails and shared documents, which may contain confidential information.

High security and high usability can be enforced by using two factor authentication as outlined below for many online services. A Student Management System also needs strong security. If two

	factor authentication is unavailable, long unique passwords should be enforced.
Long phrases as a password  Research shows that longer passwords are more secure and more usable than shorter, more complex passwords	Research shows that longer passwords are more secure and more usable than shorter, more complex passwords that may have to be changed frequently and are therefore quite possibly written down and stored. We recommend using phrases to create a memorable long password. For staff, the xkcd password generator is a good place to start. This generates a phrase of unrelated but natural language words that will produce a strong password. Some indication of how strong a password is can be obtained by using the how secure is my password website. For students it is likely that a phrase of related words will need to be used. This should be chosen in relation to their age and context. For example, young students might use their favourite colour, animal and book. You will notice that we recommend long passwords, but not necessarily complex ones. This is because a simple, yet long password is much harder to crack than a complex, but short password.
Two factor authentication  Two factor authentication requires a combination of two factors to enable authentication: something a person knows (usually a password) and something a person has	Two factor authentication requires a combination of two factors to enable authentication: something a person knows (usually a password) and something a person has (a fingerprint, app on their phone or special code sent by text message or printed and securely stored). It uses heuristics (time since last login, location, device and browser) to decide if a login attempt is suspicious. Two factor authentication is available for an increasing number of services used in schools including G Suite and Office 365,. Enabling two factor authentication for staff will significantly increase the security of their use of G Suite or Office 365. Two factor authentication has very little to no impact on usability. We recommend that it is enforced for staff, but is voluntary for students because staff are likely to own a cellphone while students may not. We suggest that if possible it is introduced to staff in a planned, gradual, managed, supportive way rather than suddenly switched on!

Single Sign On (SSO) can increase both security and usability

Many online services allow users to create and sign into their service using Google, Facebook or other services as a provider of identity

Many online services allow users to create and sign into their service using Google, Facebook or other services as a provider of identity. This should be encouraged for the following reasons:

- Fewer passwords need to be remembered than if individual accounts are created.
- The account created on the service can be logged into using only the Google or Facebook account that was used to create it.
- The Google or Facebook account used for the sign-in is likely to have good security measures in place.
- It is easy to revoke or cancel access to the service.

It is important to remember that the site that requests your Google or Facebook login never has access to your Google or Facebook password. Google or Facebook simply assert that you are a known user and pass a token to the requesting site confirming this.

There are many ways in which Single Sign On solutions can be provided. Your technical support provider may offer a Single Sign On solution.

Password Managers

Password managers are software programs that manage passwords, generally for online services.

Password managers are software programs that manage passwords, generally for online services. For the user this means that they have to remember just one very strong password to ‘unlock’ a range of passwords for different services. The database of passwords held by the password manager is encrypted and can be shared easily between devices. Password managers are an easy way to ensure that passwords are both strong and different, while the user only has to remember one ‘master’ password. Password managers combine high security with high convenience and we advocate strongly that they are used by staff.

A strategy for introducing a password manager to staff would be to get some early adopter / enthusiastic staff members to trial this and then run PD sessions for others. Password managers will need to be evaluated carefully if you wish students to use them as students often use multiple computers and this can be a complicating factor. Both online and offline password managers are available. Password managers should be encouraged on student owned devices.

Other Good Password Practices

Good practice around passwords also includes:

- Never sharing your personal password, even with a technician
- Technicians not recording passwords as they are given out
- Never writing down passwords that can be used to access sensitive data
- Always enforcing passwords to be changed at first log-in

Other ways in which passwords might be stored include Key Chain on the Mac and web browsers that save passwords. In any case, these are only as secure as the password that is required to access them so this password must be very secure (ie long and unique).

Has your account already been compromised?

The website https://haveibeenpwned.com/ allows you to enter your email address or username to find out if it has been compromised i.e. has the password published on the internet as a result of one of the various data leaks that have occurred? Typically the compromised credentials are ‘sold’ to criminal groups, rather than openly published. This means that your accounts could be used by people other than yourself, exposing your data and account to unauthorised use. If your credentials have been compromised, you should urgently change the password for any services that use it. If you have further concerns about compromised accounts then you can discuss this with Netsafe.

How are passwords most commonly compromised and how can this be avoided?

Method of Compromise	Strategies
People telling others their passwords	Encourage a culture of security where passwords are never shared with or disclosed to others.
Systems generating “easy to guess” passwords	Try to use systems that generate random passwords.
Passwords that are written down either by the user themselves or by an administrator	Consider whether passwords that are written down could end up in the hands of people that you don’t want them to.
People generating an easy to guess password for others to use	Avoid giving all users or groups of users the same initial password. Always force a password change at first log-in.
People choosing easy to guess passwords themselves	Good password creation and management practices.
Phishing attacks where spoof websites are used to collect people's credentials	Raising awareness of cyber security and the concept of phishing: ● Avoid opening or replying to spam emails ● Be cautious with emails and personal data. ● Check the website you are visiting is secure and legitimate ● Never respond to emails that request personal financial information
People send passwords by email or other insecure means	Nobody ever needs to know your password - including your technician! Once a password is written in an email it can be retrieved later so this should be avoided.
Insecure technical practices (eg allowing snooping on plain text wifi traffic or websites that do not use https to keep traffic secure)	Raising awareness of cyber security.

People deliberately stealing credentials by looking over your shoulder, using keylogger software, a hidden camera or similar	Use two factor authentication for high-risk credentials. Covering privacy as part of your Digital Citizenship programme.
Brute Force (e.g. remote) attacks	Long passwords
Hacks/exploits using Malware	Use a malware & virus checker

Useful Links

- Video explaining good password practice
- Why signing on with Google or Facebook is a good idea
- Netsafe's Blog on Two Factor Authentication
- PC World review of password managers
- Joy of Android review of password managers
- Longer passwords are more secure
- Xkcd password generator
- How secure is my password?
- Long passwords are preferable to complex passwords
- Has your account been compromised?

This guide has been produced in response to a number of specific queries about how best to manage security as it relates to passwords.
It should not be read as a recommendation or endorsement of any specific product. The Connected Learning Advisory is a Ministry of Education supported service that provides schools with technology information relevant to their queries and does not recommend one product over another.

Date Last Updated: 7th March 2018