Litton Church of England

Primary School

Password Policy

Date Reviewed: 27/04/2026
Date Approved:
Approved by:
Version: 2

Signed:

Mrs Caroline Hicks — Headteacher

Mrs Emily Noble — Chair of Governors

Review date	By whom	Summary of changes made	Date implemented
09/10/2023	C. Hicks	New policy	09/10/2023
27/04/2026	C.Hicks	Reviewed and updated	27/04/2026

Password Policy

Information by the National Cyber Security Centre

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Password use is mostly due to the surge of online services, including those provided by government and the wider public sector, and the massive growth in use of personal computers, smartphones and tablets. Passwords are often seen as an easily-implemented, low-cost security measure as they do not require special hardware, with obvious attractions for managers within enterprise systems.

However, this proliferation of password use, and increasingly complex password requirements, places an unrealistic demand on users. Inevitably, users will devise their own coping mechanisms to cope with 'password overload'. This includes re-using the same password across different systems, using simple and predictable password creation strategies, or writing passwords down where they can be easily found. Attackers exploit these well-known coping strategies, leaving your staff and organisation vulnerable.

How are passwords discovered?

- Attackers use a variety of techniques to discover passwords, exploiting a range of social and technical vulnerabilities. These include:
- tricking someone into revealing their password via social engineering (including phishing and coercion)
- using the passwords leaked from data breaches to attack other systems where users have used the same password
- password spraying (using a small number of commonly-used passwords in an attempt to access a large number of accounts)
- brute-force attacks (the automated guessing of large numbers of passwords until the correct one is found)
- theft of a password hash file, where the hash can be broken to recover the original passwords
- 'shoulder surfing' (observing someone typing in their password)
- finding passwords which have been stored insecurely, such as sticky notes kept close to a device, or documents stored on devices
- manual password guessing (perhaps using personal information 'cribs' such as name, date of birth, or pet names)
- intercepting a password (or password hash) as it is transmitted over a network
- installing a keylogger to intercept passwords when they are entered into a device

These techniques are widely available and documented on the internet, and many use automated tools requiring only moderate technical skills.

Here are steps to make your passwords effective at Litton Primary School.

1. **Use multi-factor authentication (MFA) for important accounts**

One of the most effective ways of providing additional protection to a password protected account is to use MFA. Accounts that have been set up to use MFA require a second factor, which is something that you (and **only** you) can access. This could be a code that is sent to you by text message, or that is created by an app, so even if an attacker discovers a password, they won't be able to access the associated account without also compromising the other factor. MFA is best used where there may be additional risk (such as logging into an account on a new device, internet facing systems or for priority accounts).

2. **Use throttling or account lockout**

Password systems can be configured so that there is a progressively increasing time delay between successive login attempts - a technique known as 'throttling'. This restricts the number of guesses an attacker can attempt while giving users multiple opportunities to remember their password. An alternative is account lockout, where a user only has a fixed number of attempts to enter their password before their account is locked.

- Throttling is preferred, because account lockout can leave legitimate users unable to access their accounts, and requires access to an account recovery method.
- Account lockout can provide an attacker with an easy way to launch a denial of service attack, particularly for large online systems.
- If using account lockout, we recommend you allow between 5 and 10 login attempts before the account is frozen, to avoid accidental lockout.
- Litton Primary School uses DNS filtering system for security monitoring to defend against brutal attacks.
- Weekly reports are sent to the Safeguarding team and the Business Manager monitoring the number of blocked security threats and requests to access different websites and accounts.

3. **Protect all passwords**

Passwords need to be protected within your system, even if the information on the protected system is relatively unimportant. Reuse of passwords means that an attacker can use this information to attempt to access more important accounts, where further damage can be done.

- Ensure that all corporate web apps requiring authentication use HTTPS.
- Protect any access management systems you manage.
- Protect access to user databases.
- Prioritise privileged and vulnerable accounts such as administrators, cloud accounts and remote users.
- Change all default passwords when activating an account for the first time.

4: Help users cope with password overload

Staff/Users have traditionally been told to remember passwords, and to not share them, re-use them, or write them down. The problem with this is that the typical user has dozens of passwords to remember – not just yours. To cope with this overload, users resort to workarounds, such as reusing passwords, insecure storage or predictable passwords

Don't enforce regular password expiry. Regular password changing harms rather than improves security. Many systems will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user and there are costs associated with recovering accounts.

Forcing password expiry carries no real benefits because:

- the user is likely to choose new passwords that are only minor variations of the old
- stolen passwords are generally exploited immediately
- resetting the password gives you no information about whether a compromise has occurred
- an attacker with access to the account will probably also receive the request to reset the password
- if compromised via insecure storage, the attacker will be able to find the new password in the same place

Instead of forcing expiry, you should counter the illicit use of compromised passwords by:

- ensuring an effective movers/leavers process is in place, e.g. when a member of staff leaves, all accounts are immediately blocked on the last day of their contract.
- automatically locking out inactive accounts
- monitoring logins for suspicious behaviour (such as unusual login times, logins using new devices)
- encouraging users to report when something is suspicious to the Safeguarding team.

You can also mitigate the risk of compromised accounts by using MFA, which will make a compromised password less useful to an attacker. Some MFA methods (such as SMS or email notifications) can even warn the user that they have been compromised, as they will receive a code when they did not request it.

4. Training

All staff including Governors undertake annual safeguarding training. Staff are also required to undertake Cyber Security training and GDPR training (every two years).

- highlighting the risks involved in using the same passwords across home and work accounts
- helping users to create passwords that can't be easily guessed; training can emphasise the importance of avoiding personal information (such as names, dates, and sports teams)

- using the three random words technique to help users create less predictable passwords
- training staff how to use password managers (if you're using them), including features such as the password generator

In summary

There are a number of ways you can help your staff to manage their passwords:

- permit techniques that are low risk, e.g. secure storage or remaining logged in – White Rose Maths, Read, Write, Inc Spelling.
- ensure users understand which of their accounts are of higher priority and must log out after each session, e.g. CPOMS, Arbor.
- provide users with the tools or training they need to protect these priority accounts (for example MFA, ensuring staff have logged out)