Ecclesall Primary School
High Storrs Road, Sheffield, S11 7LG
Headteacher: Mrs Emma Hardy
enquiries@ecclesall.sheffield.sch.uk
www.ecclesallprimary.co.uk

Document Adopted By Governing Body	
Date Document Adopted By Governing Body:	March 2026
Signed (Chair):	Kevin Corke
Date:	March 2026
Head Teacher Print Name:	Emma Hardy
Date of Next Review:	March 2027

ICT Password Policy

2026-27

Document Owner and Approval

Ecclesall Primary School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff within the school website: https://ecclesallprimary.co.uk/

Signature: Date:

School Password Policy

1. Introduction

The purpose of this policy is to protect school data, devices, and resources from unauthorized access. In accordance with UK GDPR and the Data Protection Act 2018, this school is committed to maintaining an appropriate level of security by implementing realistic, effective password management practices.

2. Scope

This policy applies to all "users" of school technical systems, including:

- **Staff** (including managers, contractors, and volunteers).
- **Pupils** (KS2 and upwards).
- **Governors**.

3. Password Creation: The "Three Random Words" Strategy

To ensure passwords are both secure and memorable, the school adopts the NCSC "Three Random Words" approach.

- **Length over Complexity:** Users should create a strong password by combining three random, unrelated words (e.g., apple-guitar-cloud).
- **Avoid Predictability:** Do not use common patterns (like "123" or "Password") or personal information (names, birthdays, or pet names).
- **Special Characters:** You can make your three-word password even stronger by adding numbers or symbols (e.g., Apple!Guitar4Cloud), but the priority is **length**.
- **Separate Email Password:** Staff must use a unique, strong password for their school email account that is not used for any other service.

4. Password Management & Security

To reduce the "password burden" and prevent users from writing passwords down, the school follows these technical and behavioural guidelines:

- **Save Passwords in Browsers:** Users are encouraged to save passwords in their browser when prompted. This is safer than re-using the same password across multiple sites.
- **Multi-Factor Authentication (MFA):** MFA (also known as 2-Step Verification) should be enabled on all critical accounts, especially staff email and remote access systems. This provides an extra layer of protection even if a password is stolen.
- **Changing Passwords:** In line with NCSC guidance, the school **does not** require regular, forced password changes (e.g., every 90 days). Passwords should only be changed if there is a suspicion of compromise.
- **Default Passwords:** All default vendor passwords on new hardware or software must be changed before the system is deployed.

5. User Responsibilities

Staff and Governors

- **Confidentiality:** Never share your password with anyone, including IT support or colleagues.
- **Observation:** Be mindful of "shoulder surfing"—ensure others cannot see you typing your password.
- **Reporting:** Immediately report any suspected breach or phishing attempt to the Designated Safeguarding Lead (DSL) or IT lead.

Pupils (KS2 and Upwards)

- **The Agreement:** Pupils must agree to keep their passwords private and not share them with friends.
- **Memorability:** Use three random words that are easy to remember but hard for others to guess.

Pupils (EYFS / KS1)

- For younger children, simplified login methods (such as picture-based logins or single-word passwords) may be used under teacher supervision.

6. School Responsibilities

- **Technical Controls:** The school will implement "account lockouts" after a set number of failed login attempts (e.g., 10 attempts) to prevent brute-force attacks.
- **Training:** Staff and pupils will receive regular awareness training on how to spot phishing emails and how to create secure passwords.
- **System Design:** The school will strive to implement Single Sign-On (SSO) where possible to reduce the number of passwords users need to remember.

7. Policy Review

This policy will be reviewed annually or in response to updated guidance from the NCSC to ensure it remains "state of the art" and effective against evolving cyber threats.