SCHOOL PASSWORD SECURITY POLICY	
DATE OF REVIEW: Autumn 2024	
DATE OF NEXT REVIEW: Spring 2026	
TO BE REVIEWED BY: Resources Committee	

Introduction

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

Responsibilities

The management of the password security policy will be the responsibility of the School Leadership Team.

All adult users (and young people as appropriate) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the School Leadership Team who will keep an up to date list.

Users will change their passwords on a regular basis as deemed appropriate.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety policy and Password Security policies
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's Password Policy:

- in ICT and / or online safety lessons
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights will be recorded by the ICT co-ordinator (or delegated to a representative of Computeam (the school's ICT provider) or the System Manager (SIMS).

Children will be provided with a username and password as appropriate. The computing curriculum policy is that children incrementally come to understand what constitutes a secure password.

The following rules apply to the use of password

- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *requests for password changes should be authenticated by the School Leadership Team Computeam to ensure that the new password can only be passed to the genuine user*
- *the use of google password manager is encouraged, to avoid the writing down of passwords. Where passwords are used rarely and cannot be saved by a password management system, they will be kept in a locked drawer.*

The computing lead and the school business manager are superadmins for google workspace and for office365. A further account is available for use by the Headteacher or other nominated senior leader and is kept in a secure place (eg school safe).

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.