Langham Village School Password Policy

Introduction

The school will be responsible for ensuring that the school infrastructure / 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.
- Logs are maintained of access by users and of their actions while users of the system.
- A safe and secure username / password system is essential if the above is to be established and will apply to all school computer systems, including email and online learning websites.

Responsibilities

The management of the password security policy will be the responsibility of the Head teacher and the network manager/ technology support. All adults and pupils in Key Stage 2 will have responsibility for the security of their username and password. Adults and pupils in KS2 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. In Key Stage 1 class logins will be used but monitored by the class teachers, with any concerns being passed on to the Computing subject leader or Head teacher.

Passwords for new users and replacement passwords for existing users can be allocated by the ICT Solutions.

Training / Awareness

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

- At induction.
- Through the school's e-safety policy and this password security policy.

- Through the Acceptable Use Agreement Pupils will be made aware of the school's password policy.
- In Computing, PSHE or e-safety lessons.
- Through the Acceptable Use Agreement Policy Statements.

The following rules apply to the use of passwords for adults:

- Passwords must meet the 'good' or 'strong' level according to Google Apps for Education criteria.
- The password should be a minimum of 8 characters long.
- Must include at least one uppercase character, lowercase characters,numbers, at least one special character.
- Passwords shall not be displayed on screen or on walls etc.
- Requests for password changes should be made in person to the Head teacher so the request can authenticated to ensure that the new password can only be passed to the genuine user.

The "master / administrator" passwords for the school system are kept securely by the school's technical support and Head teacher.

Security incidents related to this policy

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 reviewed annually in response to changes in guidance.

Reviewed: Sept 2025
Due for review: Sept 2027

Signed: Polly Kossowicz Head teacher