Kirk Langley Church of England Primary School

Password Policy

Kirk Langley is a Church of England Primary School and our family believe that 'Every Child Can Shine.' Our visions and values, built on the living Gospel of Christ within daily life, are at the core of everything we do. They underpin our teaching and learning and provide an environment which prepares our pupils in being respectful, confident, thriving citizens.

Daniel 12:3
'Those who have insight will shine brightly like the brightness of the expanse of heaven, and those who lead the many to righteousness, like the stars forever and ever.'

We aim to provide a thriving, inspiring and stimulating learning environment where children achieve the very best they are capable of because all the staff value their different learning styles. Kirk Langley Church of England Primary School is committed to Christian values where children, parents/carers and our community know us by our actions.

Within a Christian ethos we aim to:

- Promote a positive attitude to life-long learning, nurturing the development of self-esteem; leading to aspirational, independent learners that are prepared to be challenged and take risks in a diverse and ever changing world.
- Provide the children with valuable experiences and opportunities, through a broad, balanced and exciting curriculum, where learning is purposeful and engaging.
- Use a variety of teaching strategies and resources effectively and creatively; encouraging each child to progress and attain to the highest possible standards, in relation to their age and ability.
- Strongly believe in the partnership of parental involvement in the education of our pupils.

- Demonstrate and foster respect for ourselves and others within the school, local community and the global community.
- Respect the belief of others and celebrate cultural diversity.
- Encourage spiritual and moral values.
- Explicitly promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs through a 'living' curriculum.
- Value each child as an individual within the school and respect personal beliefs.

1. **Purpose:**

   This policy sets out how passwords must be created and managed to protect school IT systems , data and personal information in line with DFE Cyber Security Guidance.

2. **Scope:**

   This policy applies to all staff, governors, and anyone accessing school systems (email, Arbor MIS,Google/Microsoft accounts, learning platforms).

3. **Password Standards:**

   3.1 Password Creation –

   All accounts must use strong, unique passwords that are:

   - At least 12 characters long
   - A mix of uppercase and lowercase letters
   - Include numbers and symbols
   - Not based on personal information (Do not include names, birthdays, school name)
   - ***Example compliance format: Lion!Turtle42$Forest***

4. **Password Storage**:

   Store Passwords with security

   Do not save passwords in browsers without encryption

5. **Password Change Rules:**

   Passwords must be changed when:

   - A user confirms a possible compromise
   - An IT administrator requests it
   - A staff member leaves employment
   - Regular forced changes are **not required** if passwords remain secure and uncompromised

6. **Account Lockout:**

   To prevent guessing attacks:
   Accounts are locked after 3 fail login attempts
   Unlock by ICT team or authorised administrator

7. **Multi-Factor Authentication:**

   Multi-factor authentication **must be enabled** for:
   Staff email accounts
   Admin access to MIS, Office 365, Google Workspace
   Any system with sensitive data

   Acceptable MFA methods

8. **Shared Accounts:**

   - Shared logins are not permitted unless essential and controlled.
     If used:
   - Password stored in secure password manager
   - Owner assigned
   - Activity logged

9. **Educating Users:**

   All staff and volunteers must:

   - Attend annual password and security training
   - Report suspicious emails or login attempts immediately to HT/Office Staff and they will escalate to DCC.

10.Administrative Controls:

IT Manager/HT/Admin Staff:

- Review accounts x2 minimum per academic year
- Remove access when staff leave
- Ensure password manager and MFA

11.Compliance:

Failure to follow this policy may result in restricted access.