Therefore, encourage one another and build each other up, just as in fact you are doing”

1 Thessalonians 5:11

Thatcham Park C.E. Primary & Nursery School,

Password Policy

Our Christian values underpin our ethos; every child is valued and encouraged to achieve their full potential. Every member of our school community is encouraged to respect and value each other. We want our children to learn to understand and respect our common humanity, diversity and differences so that they can go on to form the effective, fulfilling relationships that are an essential part of life and learning.

1. Christian Vision and Context

At Thatcham Park Church of England Primary and Nursery School, our theologically rooted Christian vision affirms the dignity, worth and flourishing of every person, created in the image of God. We seek to ensure that our use of digital technology supports safe, wise and responsible living, enabling pupils and adults to learn and work securely.

This policy sets expectations for password security and account authentication to protect people, information and systems.

This policy reflects our commitment to wisdom, community and dignity and supports safeguarding by protecting personal data, school systems and digital access.

2. Purpose

This policy sets out how passwords and account authentication are managed across the school to protect pupils, staff, governors and sensitive information.

The policy aligns with:

- Department for Education (DfE) Digital and Technology Standards for Cyber Security.
- National Cyber Security Centre (NCSC) guidance on password management.
- UK GDPR and Data Protection legislation.
- School safeguarding responsibilities.

3. Scope

This policy applies to:

- Staff
- Governors
- Volunteers
- Contractors
- Pupils who access school systems

The policy applies to all school-managed systems including:

- Microsoft 365
- Network accounts
- Bromcom MIS
- Filtering and monitoring systems
- Safeguarding systems
- Finance systems
- Remote access services
- Administrative platforms
- External systems used by the school, including DfE services, Wonde and other authorised educational services

Where external services require separate credentials, users must follow the password requirements of those systems whilst adhering to the principles outlined in this policy.

4. Principles of Secure Authentication

The school follows modern, evidence-based cyber security guidance. This recognises that:

- Long passwords and passphrases are generally more secure than complex but short passwords.
- Forcing routine password changes can reduce overall security.
- Strong authentication is achieved through a combination of good password practice, appropriate technical controls and user awareness.
- Security controls should be proportionate to risk.
- Access should be granted using the principle of least privilege.
- Single Sign-On (SSO) should be used wherever practical to reduce password fatigue and credential sprawl.
- Multi-factor authentication (MFA) should be used wherever systems support it and where practical arrangements can be provided.
- Priority will be given to safeguarding, finance, administrator and other privileged accounts.
- Staff will not normally be required to use personal devices for MFA. Where MFA is required, reasonable alternatives will be considered.
- Authentication services and providers must meet the school's data protection requirements.

5. Password Standards

All users must create passwords which are difficult for others to guess and easy for them to remember.

Password requirements are:

- Passwords should normally be at least 12 characters long.
- Users are encouraged to use passphrases consisting of three or more unrelated words.
- Mandatory complexity rules such as symbols, mixed case or numbers are not routinely required unless dictated by a specific system.
- Common, compromised or easily guessed passwords must not be used.
- Passwords must not contain personal information such as dates of birth, pet names etc.
- Passwords must never be shared with another person.
- Where passwords need to be recorded, they should be stored securely and separately from the system they protect.
- Staff are encouraged to use approved password management tools, particularly where multiple credentials are required across school systems and approved third-party platforms. This supports the use of strong, unique passwords without creating unnecessary burden on users.

Examples of Strong Passwords

- PurpleTrainRiverWindow
- HappyCoffeeGardenHorse
- BakingRiverTigerFriday

6. Password Expiry and Routine Changes

The school does not routinely require password changes solely because a period of time has passed.

Current evidence indicates that frequent password expiry can lead users to:

- Create predictable password variations.
- Select weaker passwords.
- Record passwords insecurely.

Passwords may, however, require periodic renewal where this is mandated by a particular system, supplier or security control.

The school's preferred approach is to promote:

- Strong passphrases
- Secure account management
- User awareness
- Appropriate use of MFA
- Rapid response to suspected compromise

7. When Passwords Must Be Changed

Passwords must be changed immediately if:

- An account is suspected of being compromised.
- A password has been disclosed to another person.
- Suspicious activity has been identified.
- Directed by the Headteacher, Local Authority or IT provider following a cyber security incident.
- A password reset is required.

8. Additional Security Measures

To strengthen account security, the school may implement:

- Account lockout following repeated failed login attempts.
- Blocking of commonly used or compromised passwords.
- Secure password reset procedures.
- Monitoring and audit information available within school systems to support investigation of security incidents.
- Single Sign-On solutions where appropriate.
- Multi-factor authentication on supported systems.

The school recognises that some systems provide different levels of security functionality and controls will therefore vary according to the platform involved.

9. Multi-Factor Authentication (MFA)

Multi-factor authentication provides an additional layer of security beyond a password alone.
The school:

- Encourages the use of MFA where supported by the platform.
- Prioritises MFA for administrator, safeguarding, finance and other higher-risk accounts.
- Encourages staff to adopt MFA on supported systems where practical.
- Recognises that the use of personal devices for MFA is voluntary.
- Where MFA is required to secure a system, the school will consider reasonable alternative authentication methods where these are technically and financially viable.
- Will review emerging technologies and practical solutions as they become available.

Where systems contain safeguarding, financial, personnel or other sensitive information, MFA will be prioritised as part of the school's risk-based approach to cyber security.
The school does not access personal information stored on a device used voluntarily for MFA purposes.

10. Privileged Accounts

Accounts with elevated permissions present greater security risks and require additional safeguards.
Privileged users should:

- Use administrator accounts only when undertaking administrative activities.

- Use standard user accounts for routine day-to-day work whenever possible.
- Follow any additional security requirements attached to those accounts.
- Use MFA where supported and practical.

Administrative rights should be reviewed regularly to ensure they remain necessary.

11. Password protected documents

The school recognises that it may sometimes be necessary to encrypt documents with passwords. This is most likely to occur when the document contains sensitive information and needs to be sent via email. When this is required, the password for the document should be sent in a separate message to the document itself. The sender should ideally not use the word “password” in the subject or the email body as hackers will search for this term if they gain access to an inbox. Instead, a phrase like “access for {document name}” is preferable.

12. Joiners, Movers and Leavers

Joiners

- Accounts are created through approved procedures.
- Temporary passwords must be changed on first use.
- Appropriate access permissions are assigned according to role.

Movers

- Access permissions are reviewed when roles change.
- Unnecessary permissions are removed promptly.

Leavers

- Accounts are disabled on or before the last working day.
- Active sessions are terminated.
- Access to connected services is removed.
- Authentication methods and tokens are revoked where applicable.

13. Roles and Responsibilities

Headteacher and Senior Leadership Team
Responsible for:

- Approving this policy.
- Ensuring appropriate resources are available.
- Monitoring compliance.

IT Support Provider
Responsible for:

- Implementing technical controls.
- Managing accounts securely.
- Providing advice on security risks and improvements.

All Users
Responsible for:

- Protecting their passwords.
- Following this policy.
- Reporting suspected compromise or security concerns promptly.
- Completing relevant cyber security training.

14. Data Protection and Privacy

Authentication information is processed in accordance with:

- UK GDPR
- Data Protection Act 2018
- School Data Protection Policies

Where staff voluntarily use personal devices for MFA:

- The school does not access personal content held on the device.
- Authentication information is used solely to secure school systems.
- Appropriate privacy information will be provided where required.

15. Training and Awareness

The school recognises that staff awareness is an important part of cyber security. Staff will receive appropriate training covering:

- Password security
- Phishing and social engineering
- Safe use of school systems
- MFA awareness
- Reporting cyber incidents

Staff with administrative responsibilities may receive additional role-specific training.

16. Monitoring, Review and Compliance

This policy will be reviewed annually or sooner if:

- Cyber security guidance changes.
- Technical arrangements change significantly.
- A significant cyber incident occurs.

17. Governor Assurance

The Governing Board recognises that cyber security arrangements must be proportionate to the school's size, infrastructure and available resources. The school therefore adopts a risk-based approach to authentication, prioritising stronger controls such as MFA for higher-risk systems and accounts whilst balancing operational practicality, staff wellbeing and legal considerations relating to the use of personal devices.

Failure to comply with this policy may result in access restrictions and may be addressed through appropriate school procedures.