Llanhari Primary

Password Policy

Llanhari Primary
Version: 1
Date of Policy Approval: 16th October 2025
Review Date: Autumn 2026
Author: Emma Coates, Head Teacher
Local Authority: Rhondda Cynon Taf

1.0 Document Control and Approval

1.1 Document Information

This Password Policy sets out the standards, procedures, and responsibilities for managing passwords at Llanhari Primary. It is designed to ensure the security of digital systems and personal data, in compliance with statutory requirements and best practice guidance. The policy is reviewed regularly to ensure it remains current and effective in response to evolving threats and educational needs.

1.2 Approval and Review History

This policy has been formally approved by the Headteacher on 18th October 2025. The review schedule is set at annual intervals, or sooner if required by changes in legislation, statutory guidance, or best practice. All amendments and updates are recorded in the Policy Review Log (see Appendix 10.5).

1.3 Policy Availability and Accessibility

The Password Policy is available in both Welsh and English to ensure accessibility for all members of the school community. Copies are provided in accessible formats upon request, including large print, audio, or simplified versions for those with additional learning needs (ALN). The policy is published on the school website and is available from the school office. Staff, learners, parents/carers, and third-party users are informed of the policy's existence and their right to access it.

2.0 Policy Statement and Purpose

2.1 Policy Statement

Llanhari Primary is committed to safeguarding the digital wellbeing of its community by ensuring robust password security across all school systems.

Passwords are a fundamental component of our approach to data protection, online safety, and digital competence. We recognise that effective password management is essential to protect personal data, maintain the integrity of our digital infrastructure, and uphold our statutory responsibilities under Welsh and UK law.

2.2 Purpose and Scope

The purpose of this policy is to establish clear standards and procedures for the creation, management, and protection of passwords used to access school systems and data. The policy aims to:

- Protect digital systems, personal data, and user accounts from unauthorised access and cyber threats.
- Promote safe, responsible, and inclusive digital practices among staff, learners, and the wider school community.
- Support compliance with statutory and regulatory requirements, including safeguarding and data protection.

This policy applies to all individuals who access school systems, including:

- All staff (teaching, support, administrative, and leadership)
- All learners (pupils and students)
- Governors
- Parents/carers and authorised third-party users (e.g., contractors, external service providers)

3.0 Legislative and Regulatory Context

3.1 Statutory and Regulatory Requirements

The management of passwords at Llanhari Primary is governed by the following key legislation and statutory guidance:

- **Data Protection Act 2018 (incorporating UK GDPR):** Requires the protection of personal data through appropriate technical and organisational measures, including secure password practices (Article 32).
- **Education Act 2002:** Places a duty on schools to safeguard and promote the welfare of learners, which includes secure access to digital systems.
- **The Education (Pupil Information) (Wales) Regulations 2011:** Sets requirements for the management and protection of pupil information.
- **Welsh Government Guidance:** "Keeping Learners Safe" and "Information Management and Data Protection" outline the responsibilities of schools in safeguarding and data security.
- **Prevent Duty Guidance for England and Wales:** Requires schools to have measures in place to protect learners from online risks, including unauthorised access.

- **Information Commissioner's Office (ICO):** Provides guidance on IT security and data breach management.
- **National Cyber Security Centre (NCSC):** Offers best practice for password creation, management, and incident response.
- **Hwb (Welsh Government's digital learning platform):** Sets standards for information security and digital safety in schools.

3.2 Inspection and Compliance Frameworks

Estyn, the inspectorate for education and training in Wales, assesses schools against the Inspection Area 4: Care, support and guidance. This includes evaluation of safeguarding, data protection, and online safety measures. Schools must demonstrate:

- Existence and implementation of a robust password policy
- Staff and learner awareness of password security
- Regular review and updating of password procedures
- Secure management of user accounts and access rights

Compliance with ICO, NCSC, and Hwb standards is essential for meeting inspection requirements and ensuring the ongoing safety and security of the school community.

4.0 Roles and Responsibilities

4.1 Governing Body and Senior Leadership

The Governing Body and Senior Leadership Team at Llanhari Primary are responsible for overseeing the implementation, compliance, and regular review of the Password Policy. Their duties include:

- Ensuring the policy is fully compliant with statutory and regulatory requirements
- Allocating resources for staff training, technical support, and policy review
- Monitoring the effectiveness of password management across the school
- Supporting a culture of digital safety and responsibility

Senior leaders must ensure that all staff, learners, and stakeholders are aware of the policy and understand their roles in maintaining password security.

4.2 ICT/Data Protection Lead

The ICT/Data Protection Lead (or designated member of staff) is responsible for the day-to-day management of password security, including:

- Implementing password standards and procedures across all systems

- Monitoring compliance and investigating incidents of password compromise
- Managing password reset and account recovery processes
- Providing guidance and support to staff, learners, and parents/carers
- Maintaining records of password-related incidents and breaches

The ICT/Data Protection Lead acts as the primary point of contact for password security issues and works closely with the Senior Leadership Team to ensure ongoing compliance and improvement.

4.3 Staff Responsibilities

All staff are required to adhere to the password protocols outlined in this policy. Specific responsibilities include:

- Creating strong, unique passwords for all school accounts and systems
- Never sharing passwords with others or writing them down in accessible locations
- Reporting suspected password breaches or compromises immediately to the ICT/Data Protection Lead
- Supporting learners in understanding and applying password security principles
- Participating in regular training and awareness sessions

Staff must model good password practices and contribute to a culture of digital safety within the school.

4.4 Learner Responsibilities

Learners are expected to:

- Create passwords that are strong, memorable, and not easily guessed
- Keep their passwords confidential and never share them with others
- Report any concerns about password security to a trusted member of staff
- Engage with digital competence lessons that include password management

Age-appropriate guidance is provided to ensure learners understand the importance of password security and how to manage their passwords safely. Support is available for learners with ALN to ensure equitable access to digital systems.

4.5 Parents/Carers and Third-Party Users

Parents/carers and authorised third-party users play a vital role in supporting password security by:

- Encouraging good password practices at home

- Supporting learners in managing their passwords responsibly
- Reporting any concerns about password security to the school
- Adhering to school password protocols when accessing school systems

The school provides guidance and resources to help parents/carers understand their role in maintaining digital safety.

5.0 Password Standards and Procedures

5.1 Password Creation Requirements

All passwords used to access school systems must meet the following standards:

- **Minimum Length:** Passwords must be at least [minimum number, e.g., 12] characters long, in line with NCSC and Hwb recommendations.
- **Complexity:** Passwords should include a mix of letters, numbers, and symbols, but the emphasis is on creating memorable passphrases rather than complex strings.
- **Memorable Passphrases:** Users are encouraged to use longer, memorable phrases (e.g., "BlueDragonRunsFast!") rather than single words or easily guessed combinations.
- **Prohibited Content:** Passwords must not contain personal information (such as names, birthdays, or addresses), common words, or sequences (e.g., "123456", "password").
- **Uniqueness:** Each password must be unique to the account and not reused across different systems.

Guidance and examples are provided to help users create strong passwords (see Appendix 10.2).

5.2 Password Management and Storage

To maintain the security of passwords:

- Passwords must never be written down in accessible locations or shared with others.
- Passwords must not be stored in plain text or transmitted via insecure channels (e.g., email, messaging apps).
- Where appropriate, staff may use approved password managers to securely store and manage passwords.
- Learners are supported in developing strategies for remembering their passwords, including the use of passphrases and secure hints.

The school provides training and resources to help all users understand safe password storage practices.

5.3 Password Change and Reset Procedures

Passwords should be changed:

- Immediately if there is any suspicion or evidence of compromise
- As part of secure account recovery processes
- Not routinely or at arbitrary intervals, in line with updated NCSC guidance

Password reset procedures must include robust identity verification to prevent unauthorised access. Staff and learners are informed of the steps to take if they forget their passwords or suspect a breach.

5.4 Multi-Factor Authentication (MFA)

Where possible, multi-factor authentication (MFA) is implemented for staff accounts and any accounts with access to sensitive data. MFA adds an additional layer of security by requiring a second form of verification (e.g., a code sent to a mobile device) alongside the password.

The school monitors statutory guidance and best practice for MFA implementation and updates procedures as required. Guidance is provided to staff and learners on how to use MFA effectively.

5.5 Account Lockout and Recovery

To protect against unauthorised access:

- Accounts are automatically locked after a defined number of failed login attempts ([school-defined threshold]).
- Locked accounts can be recovered through a secure process involving identity verification and password reset.
- The ICT/Data Protection Lead oversees account recovery and ensures that all procedures are followed to maintain security.

Users are informed of the steps to take if their account is locked and how to regain access safely.

6.0 User Education and Awareness

6.1 Staff Training

All staff receive regular training on password best practices, cyber security, and statutory responsibilities. Training covers:

- The importance of strong, unique passwords
- How to create and manage passwords securely
- Recognising and responding to password-related threats
- The role of passwords in safeguarding and data protection

Training is updated in response to changes in guidance and emerging threats. Records of staff training are maintained as evidence of compliance.

6.2 Learner Education

Password security is integrated into the Digital Competence Framework (DCF) and delivered through age-appropriate lessons. Learners are taught:

- Why passwords are important for protecting personal information and digital systems
- How to create memorable, secure passwords
- The risks of sharing passwords or using weak passwords
- Strategies for remembering passwords safely

Inclusive teaching approaches are used to ensure that all learners, including those with ALN, can access and understand password security concepts.

6.3 Parent/Carer Engagement

Parents and carers are provided with information and guidance on supporting password security at home. This includes:

- Advice on helping learners create and manage passwords
- Information on the risks of weak or shared passwords
- Guidance on reporting concerns to the school

The school communicates regularly with parents/carers through newsletters, workshops, and online resources to promote a shared approach to digital safety.

7.0 Inclusion, Accessibility, and Wellbeing

7.1 Support for Additional Learning Needs (ALN)

The school recognises that some learners may require additional support to manage passwords. Adaptations include:

- Simplified password requirements for younger learners or those with ALN, balanced with security needs
- Use of visual aids, password cards, or secure hints (not the password itself)
- One-to-one support from staff or learning assistants
- Regular review of password practices to ensure accessibility

Staff are trained to identify and support learners who may struggle with password management, ensuring equitable access to digital systems.

7.2 Language and Cultural Considerations

The Password Policy and all related guidance are available in both Welsh and English. The school respects the linguistic and cultural diversity of its community by:

- Providing resources and support in the preferred language of learners, staff, and parents/carers
- Ensuring that examples and teaching materials are culturally relevant and inclusive
- Promoting digital safety as part of the school's commitment to equality and diversity

7.3 Wellbeing and Digital Citizenship

Password security is promoted as part of wider digital citizenship and online wellbeing. The school encourages:

- Positive digital behaviours, including respect for privacy and confidentiality
- Awareness of the impact of password breaches on personal and community wellbeing
- Engagement with digital competence activities that foster responsible, safe, and confident use of technology

Wellbeing is prioritised in all aspects of password management, with support available for those affected by security incidents.

8.0 Incident Management and Reporting

8.1 Responding to Password Breaches or Suspected Compromise

In the event of a password breach or suspected compromise, the following procedures are followed:

- The incident is reported immediately to the ICT/Data Protection Lead or a member of the Senior Leadership Team
- The affected account(s) are secured by changing passwords and, if necessary, locking accounts
- An initial assessment is conducted to determine the scope and impact of the breach
- Steps are taken to mitigate risks, including informing affected individuals and providing support

All staff and learners are trained to recognise and report password-related incidents promptly.

8.2 Data Breach Notification and Documentation

In accordance with ICO requirements, all password breaches are documented and, where necessary, reported to the Information Commissioner's Office. The school maintains records of:

- The nature and impact of the breach
- Actions taken to secure accounts and prevent further compromise
- Communication with affected individuals and authorities

Clear communication protocols are in place to ensure that those affected are informed promptly and provided with appropriate support.

8.3 Lessons Learned and Policy Improvement

Following any password-related incident, the school conducts a post-incident review to:

- Identify the root causes and contributing factors
- Assess the effectiveness of the response
- Integrate lessons learned into policy updates and staff training

Continuous improvement is a key principle of the school's approach to password security.

9.0 Policy Review and Continuous Improvement

9.1 Scheduled Review and Update

The Password Policy is reviewed annually or sooner if required by changes in legislation, statutory guidance, or best practice. The review process includes:

- Consultation with staff, learners, parents/carers, and governors
- Assessment of emerging threats and new guidance from Welsh Government, NCSC, ICO, and Hwb
- Updates to procedures and training materials as needed

All changes are recorded in the Policy Review Log (Appendix 10.5).

9.2 Monitoring and Evaluation

The effectiveness of the Password Policy is monitored through:

- Regular audits of password practices and compliance
- Feedback from staff, learners, and parents/carers
- Analysis of password-related incidents and breaches

Findings are used to inform policy updates and improve practice across the school.

9.3 Integration with Wider Policies

The Password Policy is aligned with the school's wider safeguarding, data protection, and digital competence policies. It forms part of a comprehensive approach to digital safety and wellbeing, ensuring consistency and coherence across all areas of school life.

10.0 Appendices

10.1 Glossary of Terms

- **Password:** A secret word or phrase used to gain access to a computer system or service.
- **Passphrase:** A longer, memorable phrase used as a password, offering greater security and ease of recall.
- **Multi-Factor Authentication (MFA):** A security process requiring more than one method of verification to access an account.
- **Data Breach:** An incident where personal data is accessed, disclosed, or lost without authorisation.
- **Account Lockout:** Temporary disabling of an account after repeated failed login attempts to prevent unauthorised access.

10.2 Example Password Guidance for Learners and Staff

Creating Strong Passwords:

- Use a phrase that is easy for you to remember but hard for others to guess, e.g., "RedDragonFliesHigh!"
- Avoid using personal information, such as your name or birthday.
- Do not use common passwords like "password" or "123456".
- Change your password immediately if you think someone else knows it.

Managing Passwords:

- Never share your password with anyone, including friends or family.
- Do not write your password down where others can find it.
- Use a password manager if recommended by the school.

For Younger Learners or Those with ALN:

- Use a memorable phrase or a combination of favourite words.
- Ask for help if you have trouble remembering your password.

10.3 Training and Awareness Materials

- Sample staff training slides on password security and cyber safety
- Age-appropriate lesson plans for learners on creating and managing passwords

- Parent/carer guidance leaflet on supporting digital safety at home
- Posters and visual aids promoting good password practices

10.4 Incident Reporting Form

Password Breach/Security Incident Report

- Name of individual reporting: [Name]
- Date and time of incident: [Date/Time]
- Description of incident: [Details]
- Accounts affected: [List]
- Actions taken: [Details]
- Further actions required: [Details]
- Reported to: [ICT/Data Protection Lead/Headteacher]
- Signature: [Signature]

10.5 Policy Review Log

- Date of review: 16th October 2025
- Reviewer(s): Emma Coates
- Summary of changes: none – new policy
- Stakeholder feedback: All staff made aware of policy and good practice as part of Cyber Security training
- Next scheduled review: Autumn 2026

11.0 References

- Data Protection Act 2018 (UK GDPR)
- Education Act 2002
- The Education (Pupil Information) (Wales) Regulations 2011
- Welsh Government "Keeping Learners Safe"
- Welsh Government "Information Management and Data Protection" Guidance
- Prevent Duty Guidance for England and Wales
- Hwb "Information Security Guidance for Schools"
- Hwb "Digital Safety and Security" Resources
- National Cyber Security Centre (NCSC) "Password Guidance: Simplifying Your Approach"
- Information Commissioner's Office (ICO) "A Practical Guide to IT Security"
- Digital Competence Framework (DCF)

- Estyn Inspection Framework
- South West Grid for Learning (SWGfL) and UK Safer Internet Centre: template policies and guidance
- NCSC's "10 Steps to Cyber Security"
- DfE's "Cyber Security Standards for Schools and Colleges"