GLEBE PRIMARY SCHOOL

UNITED LEARNING ACADEMY

Password Policy

Autumn 2024-2025

Updated: Autumn 2024
New Review: Summer 2025

Approved by the Local Governing Board on 08.10.24

Signed by: Mr. James Dempster
Position: Chair of the Local Governing Body

Title	**Password Policy for Staff and Pupils**
Policy Owner	**Director of IT**
Effective Date	**January 2018**
Last Revised	**June 2023**
Next Review Date	**June 2025**

1. Scope

The policy and procedure set out in this document applies to all Trustees and Governors, and to all staff employed by United Church Schools Trust ("UCST") and United Learning Trust ("ULT") including teaching, non-teaching, fixed term, part-time, full-time, permanent, and temporary staff.

2. Overview

Usernames and passwords, sometimes referred to as 'credentials' are the predominant method of securing access to systems and resources across digital networks. A poorly chosen password may result in unauthorised access to, and exploitation of, United Learning's systems and data. It is the duty of United Learning and all those responsible for overseeing its systems, to implement a secure password policy locally and at the centre. There are three main risks which this policy attempts to mitigate:

- **Data breach:** Unauthorised access to school or Group systems could result in losing control of data and breaching the General Data Protection Regulation (GDPR). Failure to adhere to GDPR could lead to individual and corporate fines, unlimited compensatory payments, and reputational damage.
- **Child Protection:** Unauthorised access to school or Group systems could place children at risk, create embarrassment or otherwise invade their right to privacy.
- **Operational disruption:** Unauthorised access to school or Group systems could result in these systems or their data being made unavailable, impacting significantly on schools' ability to operate.

3. Purpose

The purpose of this policy is to define a strong password standard, establish best practice in the protection of those passwords and when they must be changed. The intent is to strike a balance between the two extremes of 'total lock-down' and 'completely open' to set a policy which ensures security whilst not creating burdensome barriers for authorised users.

4. Staff policy

All staff who have, or are responsible for, an account that can access United Learning systems or data must passwords to protect their accounts. Passwords must not be shared and not be the same as a password used to access any other system (including personal accounts) however systems that support Single Sign On (SSO) is preferable.

5. Password/Passphrase creation

Standard user level passwords must contain a minimum of eight (**8**) characters (length should be as long as you can comfortably remember) and contain one of the following:

- **Lower case letter**
- **Upper case letter**
- **Number**

Additional guidance:

- may also contain special characters – highly recommended e.g.!"$%^&*()¬
- must not contain all or part of the user's name, username or other information known by others or easily discovered (e.g., pet or child's name, date of birth).
- Passwords should not be single words that are found in dictionaries.
- Phrases (combinations of 2-3 words) are encouraged e.g., NowPatrioticHour, add special characters to create a complex password e.g. N0wP4triot!cH0ur.
- Consider using a password manager to ensure unique passwords are used.

Passwords must not be characters or places from popular media (football club names, books, films TV programmes, etc).

Admin passwords used for accessing system level accounts should have a minimum of twelve (**12**) characters.

6. Password change

Standard user & elevated level passwords should be set to expire every 365 days.

Systems must be configured to:

- inform users when a password is due to expire and how to change it.
- prevent the re-use of passwords that have been previously used for the account.
- prevent passwords from being changed more than once per hour.

Admin passwords used by school technical staff must be set:

- to expire at (or within) sixty (**60**) days.

7. Password protection

Passwords must never be shared with anyone else, including IT Technicians, Line Managers, subordinates, or family members. There are procedures to allow assistants to access email and calendar accounts without compromising password security.

Shared accounts (e.g., 'Reception PC') must not be used.

Passwords must not be stored in plain text e.g.; in iPhone notes etc.; this includes being written down on paper.

If a user suspects that their password has been compromised, they must contact the local IT Team immediately.

8. Password resets

If a password is forgotten the user should use self-service password reset where it is available or contact the local IT Helpdesk to reset the password.

If the user is not present, a member of the local IT service may only communicate the new password using validated contact details found in the school's MIS, from HR or the employee's line manager.

Reset Passwords must be set to expire on first use so that a new password can be entered.

10. Account lockout

Account lockout should be enabled to cause an account to be locked out either for a specific period or until it is unlocked by a system administrator.

Account lockout should be triggered after five incorrect attempts for staff and KS4 pupils.

Account lockout for KS1-KS3 should be triggered between five and ten incorrect attempts.

Exceptions for students can be authorised by the Network Manager.

11. Devices

Mobile devices must be secured with a minimum 6 digit PIN/password.

School laptops and computers must be secured with valid username and password, meeting password requirements set out above.

12. Two/Multi-Factor Authentication

All users must have MFA applied to the following systems as a minimum:

System Name	Logging in on school premises	Logging in out of school	Relevant Staff
Office 365	No MFA required in school	User may be prompted to validate login via MFA approx. every 30-90 days	All staff
iTrent/ESS	MFA automatically triggered every hour	MFA automatically triggered once per hour	All staff
EIP	MFA automatically triggered every hour	MFA automatically triggered once per hour	SLT, Governors and relevant roles
Arbor / iSAMS	No MFA required in school	User prompted at every login	All staff
Access / FocalPoint	MFA automatically triggered every hour	MFA automatically triggered once per hour	SLT, Governors, Finance Leads, expense approvers

Any other systems that use Microsoft Single Sign On would be treated the same as Office 365 authentication.

For Admin level account users MFA must be enabled and required on every sign in. Service accounts with Admin privileges do not require MFA but must have a long (20+ character) and complex password.

MFA can be implemented by using an authenticator app (recommended) or with a code delivered via SMS/ phone call/code generator.

13. Pupil password policy

All pupils should be encouraged to use and understand the reasons for named accounts with appropriate passwords and advised not to share passwords with classmates or teachers.

Each account must have a unique password for each pupil. It is not necessary for primary age pupils to have complex passwords, as the sensitivity of the data in pupil accounts/systems to which they have access is likely to be low. Pupil passwords at KS3 and higher must contain a minimum of eight (**8**) characters and contain at least one each of the following:

- Number
- Lower case letter
- Upper case letter
- Special characters may be used.

Primary - pupil passwords should not be set to expire; however older pupils should be encouraged to create their own passwords.

Secondary – pupil passwords should not be set to expire except when they move up a Key Stage, to better secure examination work.

14. External contractors

External contractors must have the same policy applied to their accounts as for staff.

Contractors who are granted access to devices and systems must be included within the main O365 conditional access MFA policy.

All devices issued or used by external contractors must meet the minimum requirements for passwords as set out in **section 11**.