Shaw Education Trust

Password Policy

Procedure Originator:	Pete Potts
Approved By:	C-Suite
Queries to:	John Lavelle and Dave Orum
Review Interval:	Every 3 years or when needed
Last review:	1st September 2024 (new)

[Type here]

This policy has been equality impact assessed and we believe in line with the Equality Act 2010. It does not have an adverse effect on race, gender or disability equality.

Introduction

Securing sensitive data is becoming more and more difficult with users having access to so many devices, Wi-Fi and internet connectivity.

Single Sign on and shared accounts means a security leak on one system could allow unauthorised access to others.

Teachers and pupils have access to data, documents and systems from home, the school network via Wi-Fi from the school grounds and with cloud email and storage: a lost password could give malicious users easy access to a host of systems.

Staff and students often don’t realise the potential risks this poses and it is important that e-Safety training and guidance helps to educate both groups of users. This policy is designed to be a part of that education.

Tablets, iPads, mobile phones, cameras and home laptops often don’t support good practice with required passwords and it is important to consider the types of data held on these devices, particularly if leaving the school. own policy.

Madeley School will be responsible for ensuring that the school data and network is as safe and secure as is reasonably possible and that:

- users can only access systems and data to which they have right of access
- users should agree to an acceptable use policy
- users should be unable to access another’s files
- users must not store their passwords in plain view and staff must not write down passwords.
- access to personal data is securely controlled in line with the school’s Information Security Policy
- where possible logs are maintained of access by users and of their actions while users of the system

1. Responsibilities

1.1 All users provided with their own user accounts will have responsibility for the security of their username and password.

1.2 They must not allow other users to access the systems using their log on details and must immediately change their password and report any suspicion or evidence that there has been a breach of security.

1.3 Class accounts used for pupils should be monitored by the class teacher and pupils should only use under supervision.

1.4 New user accounts, and replacement passwords for existing users will be allocated by the ICT technician or school technician.

1.5 Staff and pupil accounts must be disabled upon leaving the school and user data deleted as appropriate.

1.6 School office staff should ensure that leavers are processed as soon as possible.

1.7 All users are advised to change their passwords occasionally to ensure systems remain secure. However, the length between changes needs to take into account the type of user and the risk to the school if unauthorised access was gained. Your password will not automatically expire. The IT team will only ask users to change their passwords on indication or suspicion of compromise.

1.8 Similarly the complexity of passwords needs to reflect the user.

1.9 Users should change passwords taking the following schedule and complexity into consideration:

- Staff passwords minimum 8 characters including the following types upper, lower, numeric
- Student passwords minimum 8 characters including the following types upper, lower, numeric
- Passwords should not be re-used for 10 consecutive password changes.
- Tablets or other devices syncing to email, cloud storage or storing data not able to meet these requirements must as a minimum use 6 digit pin codes. The mail administrator may enforce stricter requirements

2. Policy Statements

2.1 All users will have clearly defined access rights to school ICT systems.

2.2 Details of the access rights available to groups of users will be monitored and reviewed by the ICT department.

2.3 All users will be provided with a username and password.

2.4 Shared class logons for pupils may be used but the school needs to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the IT Security Policy. Use by pupils in this way should always be supervised and members of staff should never use a shared class log on for their own network access.

2.5 The following rules apply to the use of passwords:

- the account will be "locked out" following ten successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password resets for a pupil should be requested by a member of staff. Password resets for a staff accounts must be requested by the individual directly.
- where sensitive data is in use – particularly when accessed on laptops – additional forms of authentication may be enforced, e.g. two factor authentication.

Shaw
Education
Trust

Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
ST7 4DL

Twitter	@ShawEduTrust
LinkedIn	@ShawEducationTrust
Call	01782 948259
Email	info@shaw-education.org.uk
Visit	shaw-education.org.uk

Pupil & people centred

Act with integrity

Be innovative

Be best in class

Be accountable