SCHOLARS ACADEMY TRUST
STRIVING FOR EXCELLENCE

Support
Tenacity
Responsibility
Innovation
Voice
Equity

Password Policy

Date or Review	March 2023
Next Review Date	March 2025
CEO	Sam Coy
Chair of the Trust	Sarah Richards
Signed	Signed copy held centrally
Date	30/06/23

Password Policy- Scholars Academy Trust and Schools

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

- Users can only access confidential data to which they have a right of access.
- Access to personal data is securely controlled in line with the school's personal data procedures.
- Logs are maintained of access by users and of their actions while users of the system.
- There are regular reviews and audits of the safety and security of school computer systems.
- There is an oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility the IT coordinator and technicians.

Technical Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Technical Staff (or another person) and will be reviewed, at lease annually by a Senior Leader.
- Users will be made responsible for the security of their username and password, they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks and email.

- All school networks and systems will be protected by secure passwords that are regularly changed (at least once every 90 days).
- The "master/administrator" passwords for the school's systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place i.e. school safe.
- Usernames for new users will be allocated by the IT technicians. Passwords are only known by the user.
- All users (adults and children) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must

immediately report any suspicion or evidence that there has been a breach of security.

- Lost passwords are reported to technician who has responsibility to reset account.

- All documents emailed containing personal details will be password protected.

Staff Password

- All staff users will produce a password but the username will be provided by the IT technician. Who will keep an up to date record of users and their usernames.

- The password should be a minimum of 8 characters long and must include uppercase character, lowercase characters, numbers and special characters.

- The account should be "locked out" following six successive incorrect log-on attempts, the IT technician will then reset the account.

- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.

- Passwords shall not be displayed on screen.

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.

- Should not be re-used and be significantly different from the previous password.

Pupil Passwords

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

- Pupils will be taught the importance of password security.

- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- At induction
- Through the school's online safety policy and password security policy
- Through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- In lessons
- Through the Acceptable Use Agreement

Monitoring

This policy will be reviewed on a biannual basis or sooner if monitoring or other information comes to light