Laurel Avenue
Community Primary School

School Password Security Policy

Introduction

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

- *users can only access data to which they have right of access*
- *no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).*
- *access to personal data is securely controlled in line with the school's personal data policy*

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of the Computing Coordinator and Headteacher.

All users in Key Stage 2 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.

Passwords for new users and replacement passwords for existing users will be allocated by the Computing Coordinator. Any changes carried out must be notified to the manager of the password security policy.

Users will change their passwords every term and will make sure that they are significantly different from previous passwords created by the same user.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

- *at induction*
- *through the school's e-safety policy and password security policy*

- *through the Acceptable Use Agreement*

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

- *in ICT and/or e-safety lessons*
- *through the Acceptable Use Agreement*

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Coordinator and will be reviewed, at least annually, by the E-Safety Group.

All users at KS2 will be provided with a username and password by the ICT Coordinator who will keep an up to date record of users and their usernames. Users will be required to change their password every term.
Class log-ons and passwords are used for KS1 and below. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.

The following rules apply to the use of passwords:

- *passwords must be changed every term*
- *the password should be a minimum of 8 characters long and must include three of: uppercase character, lowercase character, number, special character*
- *must not include proper names*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*

Sensitive data is not to be stored on Desktop PCs or on laptops and only on encrypted data sticks provided to staff by school or on the Durham Learning Gateway.

The "administrator" passwords for the school ICT system, used by ICTSS, ICT Technician and ICT Coordinator is also available to the Headteacher and Deputy Headteacher and kept in a secure place - school safe).

Audit/Monitoring/Reporting/Review

The responsible person, ICT Coordinator, will ensure that full records are kept of:

- *User log-ons*
- *Security incidents related to this policy*

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by: E-Safety Coordinator, E-Safety Group, E-Safety Governor at regular intervals (termly).

This policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Signed: G Davison

Headteacher
Date: March 2018

Signed: C Linfoot

Chair of Community and SMSC Committee
Date: March 2018

Signed: C Linfoot

Review: March 2021