

Password Security Policy



Introduction

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 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 systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of ICT subject leader. All adult users and children 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. Children in Key Stage 1 and Foundation Stage have individual usernames with a shared password.

Policy Statements

All users will have clearly defined access rights to school systems. Details of the access rights available to groups of users will be recorded by the Computing subject leader and will be reviewed, at least annually. All users (at KS2 and above) will be provided with a username and password by the Computing subject leader who will keep an up to date record of users and their usernames. Users will be required to change their password annually (or after a user request or password infringement).

Passwords must be:

- Minimum of 5 characters long
- Contain at least a lower and upper case letter (ideally a number is included)

Children in year 3/4 use their house teams with a self-selected number e.g. Badger 7

Children in year 5/6 select their own password. (providing computing subject leader a hint)

Passwords are used for signing into the school computer system and our VLE.

Passwords for new users and replacement users will be allocated by the Computing subject leader. Where sensitive data is in use, encrypted or password protected devices will be used. The "master / administrator" passwords for the school system, used by the Computing subject leader must also be available to the Headteacher.

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.

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

- in Computing and / or online-safety lessons
- through the Acceptable Use Agreement (signed on school entry and resigned with parents on entry to Key Stage 2).

Audit /Monitoring /Reporting /Review

The responsible person (Computing subject leader) will ensure that full records are kept of:

- User IDs and requests for password changes
- 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.

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2018