**St Mary’s C of E School**

**School Password Security Policy**



**Date reviewed: July 2015**

**Signed: Headteacher:**

**Signed Chair of governors:**

**Date of next review:**

**Introduction and purpose of policy**

The school is responsible for ensuring that the 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

• logs are maintained of access by users and of their actions while users of the system

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).

This links with the school aims of:

* Provide a secure environment, physically and emotionally, in which all children are offered equal opportunities and are taught to value their own skills and abilities and those of others
* Teach courtesy, good manners and consideration of others.

**Responsibilities**

The management of the password security policy will be the responsibility the Computing coordinator and the Technical staff.

All users (adults and young people) will have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security. KS2 children will use their own individual logins and KS1 will use class logins.

Passwords for new users, and replacement passwords for existing users will be allocated by ICT 4 or by the computing coordinator. (Any changes carried out must be notified to the manager of the password security policy (above).

*Users will change their passwords at least every 6 weeks.*

*Passwords:*

* are not re-used for 6 months.
* 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 logons 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 or e-safety lessons and through school assemblies
* through the Acceptable Use Agreement

35

**Policy and Practice**

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 Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All users (at KS2 and above) will be provided with a username and password either by ICT 4, Daniel King or Lisa Spry, and they will keep an up to date record of users and their usernames. Users will be required to change their password every 6 weeks and all Internet usage can be logged through the school’s filtering system.

All uses in KS1 will use class logons and passwords to ensure that work is saved in the correct folders. When using I.C.T equipment, KS1 pupils should be supervised by members of staff at all times to ensure that any individual who may infringe the rules set out in the AUP can be identified. Users will not change their password and individual Internet usage cannot be logged on the school filtering system.

The following rules apply to the use of passwords:

*• passwords must be changed every month/term* (see earlier section under Responsibilities)

* the last four passwords cannot be re-used
* the password should be a minimum of 5 characters long and
* must include two of – uppercase character, lowercase character, number, •
* the account should be “locked out” following six 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 changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil

The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (secure large filing cabinet in Head teacher’s office).

**Audit / Monitoring / Reporting / Review**

The responsible person (ICT co-ordinator) will ensure that full records are kept of:

• User Ids and requests for password changes

• User logons

• Security incidents related to this policy

36

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 annually by the *e-safety committee group.*

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