St John's C of E Primary Academy

Password Security Policy

Author: Sarah Cockshott

Date of issue: January 2017

Review date: January 2018

Key Personnel

Principal: Sarah Cockshott

Chair of Governors: Fr Roger Gilbert

Academy Policy

Introduction

The academy will be responsible for ensuring that the *academy 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 academy's policies).
- access to personal data is securely controlled in line with the academy'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 academy ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of Network Manager and / or the Computing Co-ordinator.

All year 5+6 children and adults 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. Years 3+4, Key Stage 1 and below passwords will be known to staff. Staff are not to use the KS1 login to access the network.

Passwords for new users and replacement passwords for existing users can be allocated by ICT Network Manager. Any changes carried out must be notified to the manager of the password security policy.

Users will change their passwords every 6 months.

Training / Awareness

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

- at induction
- through the academy's e-safety policy and password security policy
- through the Acceptable User Agreement

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

- in ICT and / or e-safety lessons (the academy should describe how this will take place)
- through the Acceptable User Agreement

Policy Statements

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

All years 5+6 children will be provided with a username and password by ICT Co-coordinator / ICT Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 6 months. Group log-ons and passwords for years 3+4, KS1 and below will be provided, but need 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 policy and the AUP. 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. Academy's should also consider the implications of the development of Learning Platforms and home access on whole class log-ons and passwords

The following rules apply to the use of passwords:

- passwords must be changed every 6 months.
- the last four passwords cannot be re-used
- the password should be a minimum of 6 characters long and

- must include three of – uppercase character, lowercase character, number, special character
- 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 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 network manager / ICT Co-ordinator to ensure that the new password can only be passed to the genuine user

The "master / administrator" passwords for the academy ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. academy safe).

Alternatively, where the system allows more than one "master / administrator" log-on, the Principal or other nominated senior leader should be allocated those master / administrator rights. An academy should never allow one user to have sole administrator access).

Audit / Monitoring / Reporting / Review

The responsible person 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 and Academy 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 Officer /E-Safety Governor)* at regular intervals.

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

Policy Date:- January 2017

Review Date:- January 2018