



School Password Security Policy

Policy or procedure reference number: 020
Issue number : 1
Date: 02/10
Review date: 02/11
Responsibility for review: Curriculum
Related policies: Acceptable User Agreement

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
- 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).

Responsibilities

The management of the password security policy will be the responsibility of the school Bursar.

All users (adults and young people) 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 Denise Barkham. Any changes carried out must be notified to the manager of the password security policy (above).

Training / Awareness

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 / students 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 be provided with a username and password by Denise Barkham who will keep an up to date record of users and their usernames. Users will be required to change their password annually.

The following rules apply to the use of passwords:

- passwords must be changed every year
- passwords shall not be displayed on screen
- 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

The “administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the School Bursar and kept in a secure place (eg school safe).

Audit / Monitoring / Reporting / Review

The responsible person (Denise Barkham) 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.

(In Maintained schools) 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 the Committee Committee/Safeguarding Governor) annually.

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

End of policy.