Policy for Password Security

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 the Virtual Learning Environment (Durham Learning Gateway).

Responsibilities

The management of the password security policy will be the responsibility of the E-safety co-ordinator.

All users (adults and pupils) 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. NB. This does not apply to Key Stage 1 where Class Log Ons are provided.

Passwords for new users, and replacement passwords for existing users will be allocated by the E-safety Co-ordinator.

Supply teachers and visitors to the school who require ICT access will be allocateda username and password which provides limited access to school network.

Users will change their passwords every year.

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

- ine-safety lessons;
- through the Acceptable Use Agreements;

Policy Statements

All users (at KS2 and above) will be provided with a username and password by the E-safety Co-ordinator who will keep an up to date record of users and their usernames. Users will be required to change their passwords every year.

The following rules apply to the use of passwords:

- passwords must be changed every year;
- the last three passwords cannot be re-used;
- the password should be a minimum of 8 characters long andmust include three of the following : uppercase character, lowercase character, number or special character;
- passwordsmust not include proper names;
- 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)

The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place (eg school safe).

Audit / Monitoring / Reporting / Review

The E-safety co-ordinator 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.

NB. Durham LEA 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.

This policy will be regularly reviewed annuallyby the E-Safety Committeein response to changes in guidance and evidence gained from the logs.