Brockley Primary School

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 adult user should be able to access another staff members 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 data protection policy.
- Logs are maintained of access by users and of their actions while users of the administration systems.

A safe and secure username/password system is essential if the above is to be established and will apply to all school Computing systems, including email.

Responsibilities

The management of the password security policy will be the responsibility of the Head teacher and Computing co-ordinator.

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 system 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 the Computing coordinator and Headteacher.

Passwords for the network, email, online learning resources etc will be managed and monitored by the Computing coordinator.

Passwords for the Management Information Systems such as RM Integris, Evolve, SAP, Abacus, Purple Mash, Teachers 2 Parents, etc will be managed by the School Business Manager. Users will change their password every 90 days on the MIS system and Finance system when prompted, on the administration machines.

Any changes carried out must be notified to the manager of the password security policy as above. (Headteacher or Computing Co-ordinator.)

Passwords for school's encrypted memory sticks, which hold sensitive pupil information, are held only by the Headteacher. (See encrypted memory stick policy) No members of staff will change the passwords on their allocated memory stick, which remains the property of the school.

Training/Awareness

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

- At induction
- Through the school's e-safety policy and password security policy
- Through the Acceptable Use policy

Pupils will be made aware of the school' password policy:

- In Computing and e-safety lessons
- Through the Acceptable Use policy

Policy Statements

All users will have clearly defined access rights to school Computing systems. Details of the access rights available to groups of users will be recorded by the Headteacher and will be reviewed at least annually by the Teaching and Learning Sub Committee.

All users will be provided with a username and password by Mrs Debbie Monk – Computing co-ordinator, who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- Passwords must be changed every 90 days (Admin logins only)
- The last four passwords cannot be re-used (Admin logins only)
- 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 Mrs Debbie Monk to ensure the new password can only be passed to the genuine user.

The master/administrator passwords for the school Computing system, used by the Computing maintenance supplier must also be available to the Headteacher and Computing co-ordinator and kept in a secure place (eg head's encrypted data stick is more secure). The school should never allow one user to have sole administrator access.

Audit/Monitoring/Reporting/Review

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

- User ID's and requests for password changes
- User log-ons
- Security incidents related to this policy

In the vent 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 relation information must be given to the highest security classification and stored in a secure manner.

These records will be reviewed by the Governors as part of the Safeguarding Agenda Item at regular intervals.

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