BRINKWORTH EARL DANBY'S CE PRIMARY SCHOOL

Serving the communities of Brinkworth and Dauntsey

VISION

Believe to Achieve!

To provide a secure, happy and stimulating learning environment in which EVERYONE is valued, spiritual growth is nurtured and potential maximised.

PASSWORD POLICY

School Password Security Policy

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 ICT Coordinator and the Network Manager

All adults and pupils in Key Stage 2 will have responsibility for the security of their username and password. Adults and pupils in KS2 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. In Key Stage 1 class logins will be used but monitored by the relevant class teachers, with any concerns being passed on to the ICT Coordinator or the E-safety Coordinator.

Passwords for new users and replacement passwords for existing users can be allocated by the Network Technician

Adult users will change their passwords every 90 days, while KS2 pupils will change their passwords every year.

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, PSHE or e-safety lessons.
- Through the use of posters placed near every PC or terminal.
- Through the Acceptable Use Agreement

Policy Statements

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 by the Network Technician who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days, while KS2 pupils will change their passwords every year.

The following rules apply to the use of passwords for adults:

- Passwords must be changed every 90 days
- The password should be a minimum of 8 characters long and
- Must include three of – uppercase character, lowercase character, number, special character
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Requests for password changes should be made in person to the ICT Coordinator, E-safety Coordinator or the Head teacher so the request can authenticated to ensure that the new password can only be passed to the genuine user

The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe). (Alternatively, where the system allows more than one "master / administrator" log-on, the Head teacher or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access).

Audit / Monitoring / Reporting / Review

The responsible person Network Technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- 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 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 *E-Safety Coordinator and E-Safety Governor* at regular intervals with a minimum of once a year.

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