SHIPHAM C OF E FIRST SCHOOL
PASSWORD SECURITY POLICY

This policy should be read in conjunction with the school's E-Safety and Data Protection policies.

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 (if appropriate) any Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of the Headteacher (or Designated Data Controller).

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
- 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 Headteacher or ICT Technician.

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

- in ICT and / or e-safety lessons
- through the Acceptable Use Agreement

Policy Statements

Group/class log-ons will be used throughout the school and use of internet by pupils will always be supervised.

Pupils who use home access, email and/or VLE will be provided with a username and password and an up to date record of users and their usernames will be kept by the class teacher.

The following rules (regulated by the LA) apply to the use of passwords for staff:

- passwords must be changed every month
- the last four passwords cannot be re-used
- the password should be a minimum of 8 characters long and
- 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 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
- 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 "master / administrator" passwords for the school ICT system, used by the ICT Technician and School Secretary, must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

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

January 2013