Forres Sandle Manor (Non-Academic) Policy

Policy Title	**Password Security**
Policy Lead (Appointment (& Initials))	**Network Manager (DA)**
Date of Last Review	**September 2019**
Date of Next Review	**September 2020**

PASSWORD SECURITY

OVERVIEW

A safe and secure username/password system is essential for FSM to ensure that the school's network infrastructure is as safe and secure as is reasonably possible, and will apply to all FSM technical systems, including networks, devices, email and online resources used.

POLICY STATEMENTS

- All users will have clearly defined access rights to FSM technical systems and devices. Details of the access rights available to different categories of users will be maintained by the IT Staff and will be reviewed at least annually.

- All FSM networks and systems will be protected by secure passwords that are regularly changed.

- The *administrator* passwords for the FSM systems used by the IT staff must also be available to the Head and be kept in a secure school safe.

- All users (staff and pupils) will have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. They 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 IT Staff.

- Users will change their passwords at regular intervals as described in the staff and pupil sections below.

- Requests for password changes need to be made in person to the IT Staff to ensure that the new password is only known to the genuine user.

STAFF PASSWORDS

- All staff users will be provided with a username and password by the IT Staff who will keep an up to date record of users and their usernames.

- Password Protocol and Best Practice.
  - Password to be a minimum of 8 characters long and must include at least 3 of the following type: an uppercase character, a lowercase character, a number, a special character.

  - The password must not include proper names or any other personal information about the user that might be known by others.

  - The account will be locked out for a period of 30 minutes following 6 successive incorrect log-on attempts.

  - Passwords shall not be displayed on screen, and shall be *securely hashed* (a technical process which uses of one-way encryption).

  - Temporary passwords (used with new user accounts or when users have forgotten their passwords) shall be enforced to change immediately upon the next account log-on.

  - Passwords must be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of FSM:
    - Systems that are *inside school* and will use your FSM network password via the Single Sign-On process are …. logging on to the internal school network, Outlook Web Access, Office365, your Google login for accessing your Chromebook and Google GSuite, and other online resources making use of the Google login
    - Any other system is classed as outside FSM must have a different password. This includes SchoolBase Online, and independently accessed teaching resources.

  - Passwords must:
    - be changed every 360 days
    - have a minimum age of 1 day
    - be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used

PUPIL PASSWORDS

- All users from Year 3 will be provided with a username and password by the IT Staff who will keep an up to date record of users and their usernames.

- A class password will be used for Year 1 and Year 2.

- The password should be a minimum of 8 characters long.

- Users will be required to change their password every 360 days.

- Pupils will be taught the importance of password security in Computing lessons.

TRAINING AND AWARENESS

- It is essential that users are aware of the need for keeping passwords secure, and the risks attached to unauthorised access or data loss.

- Members of staff will be made aware of this Password Security Policy:
  - at induction
  - through FSM's E-Safety policy
  - through the E-Safety Agreement for Acceptable Use of FSM's ICT Systems

- Pupils will be made aware of FSM's password policy:
  - in lessons as part of the teaching for Computing and Internet Safety.
  - through the E-Safety Agreement for Acceptable Use of FSM's ICT Systems

AUDIT /MONITORING/REPORTING

- The Network Manager will ensure that full records are kept of:
  - User IDs and requests for password changes
  - User log-ins
  - Security incidents related to this policy

POLICY REVIEW

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