Password Policy

Adopted:	June 2021
Chair of Health and Safety Committee:	Mrs K Lincoln
Safeguarding lead Governor	Mrs K Bullivant
Designated Safeguarding Lead	Mr Fisher
Next review date:	June 2022

A safe and secure username / password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Group
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "administrator" passwords for the school systems, used by the technical staff must also be available to the Head teacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) 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 network manager.*
- *Users will change their passwords at regular intervals – as described in the staff and pupil sections below*

Staff passwords:

- All staff users will be provided with a username and password by (System administrator, Luke) who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others

- 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 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
- passwords should 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 school
- should be changed at least every 60 to 90 days
- Should not be re-used for 6 months and be significantly different from previous passwords created by the same user.

Pupil passwords

- **All users (at KS2 and above) will be provided with a username and password** (System administrator, Luke) who will keep an up to date record of users and their usernames.
- **KS1 users will be provided with a username and a generic password.**
- pupils will be taught the importance of password security through their computing curriculum

Training / Awareness

Members of staff will be made aware of the school’s password policy:

- at induction
- through the school’s online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school’s password policy:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (System administrator) will ensure that full records are kept of:

- User Ids
- Security incidents related to this policy

Acknowledgements

Oakridge Primary school acknowledges the assistance of SWGFL in providing content for this document.