BURTONWOOD C.P. SCHOOL

Password Policy

Omega Multi-Academy Trust

Contents:

Statement of intent

1. Introduction
2. Responsibilities
3. Training and Awareness
4. Policy Statements
5. Audit/Report/Review

Statement of intent

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that data is held securely. Any data breach will not be taken lightly and will be reported to the head teacher in order for any necessary further action to be taken.

This password policy is designed to ensure all data is held securely.

Signed by:

____________________ Headteacher   Date: ____________________

____________________ Chair of governors   Date: ____________________

Review date: ____________________

1. 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 using 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.

2. Responsibilities

2.1 The management of the password security policy will be the responsibility of the Head Teacher and Computing Coordinator.

2.2 All users (adults and young people) will have responsibility for the security of their username and password. They 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.

2.3 Passwords for users and replacement passwords will be managed in accordance with the table below

Platform	Initial responsibility/Admin rights	Additional Support	Period of change
Network	Omegat MAT IT Support	Marc Miller or David Lomas	Annually
Omega MAT emails	Omega MAT IT Support	Marc Miller or David Lomas	Annually
Burtonwood CP Emails	Omega MAT IT Support	Marc Miller or David Lomas	Annually
Twinkl, Hamilton trust, Master the Curriculum, White Rose Maths, Classroom Secrets	Louise Eckersley	Louise Eckersley	Annually
SIMS, Evolve, Teachers2Parents, Parent Pay (other office admin sites)	Louise Eckersley Sandra Fairhurst	Omega MAT IT Support	Annually
Reading Plus and Spelling Shed	Jessica Baker	Sarah Ignatius	Annually
Nessy	Joanne Hughes		Annually
Reading Eggs and Maths Seeds	Sarah Ignatius		Annually
Real PE	Jessica Baker		Annually
TT Rockstars	Sarah Ignatius		Annually
Seesaw	Sarah Ignatius		Annually

3. Training and Awareness

3.1 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.

3.2 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 for Staff

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

- During Digital Literacy, PSHE and/or e-safety lessons. Children will be given opportunities to explore and discuss various safety/security scenarios through recommended sites such as 'Think u know' and 'Childnet'.
- Through the Acceptable Use Agreement for Pupils

4. Policy Statements

4.1. All users will have clearly defined access rights to school Computing systems.

4.2. Details of the access rights available to groups of users will be recorded by the Head Teacher and Computing coordinator and will be reviewed at least annually by Governors.

4.3. All users will be provided with a username and password by the adult listed above.

4.4. The following rules apply to the use of passwords:

- Passwords must be changed annually (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 the Computing coordinator, Mrs Sarah Ignatius, to ensure the new password can only be passed to the genuine user.

4.5. 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 the safe).

4.6. The school should never allow one user to have sole administrator access.

4.7. The WIFI password is to be held only by IT support and Sarah Ignatius.

4.8. All users at Year 2 & KS2 will be provided with a username and password and Sarah Ignatius will keep an up-to-date record of users and their usernames. Users will be required to change their password every year and will change their initial password on their first login attempt. They may choose their own password.

4.9. For children in Year 1, the passwords will be one of 4 animals that children can spell easily to ensure accessibility is efficient and effective. As 4 passwords will inevitably result in the ability to log in as another user, members of staff will closely supervise children's use of technology in school.

4.10. For children in Reception whole class logins will be used by all children to ensure accessibility is efficient and effective. As whole class passwords will inevitably result in the inability to identify any individual who may have infringed the rules set out in the policy and the Acceptable Use Policy for Pupils, members of staff will closely supervise children's use of technology in school.

5. Audit/report/review

5.1. Sarah Ignatius will ensure that full records are kept of:

- User IDs and requests for password changes
- User logins
- Security incidents related to this policy

5.2. The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

5.3 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.

5.4 User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

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