PASSWORD SECURITY POLICY

Torfield and Saxon Mount Academy Trust

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 and GDPR policies
- 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, any Virtual Learning and Communication Environments in use, and also other curriculum and software products involving individual pupil and parent access, and other business and management software systems including staff, pupil and parent/carer data.

Responsibilities

The management of the password security policy will be the responsibility of all staff where students log on to the computer network, and the Network Manager

All adults will have responsibility for the security of their usernames and passwords for all hardware and software applications.

All pupils will be supported in taking responsibility for security of usernames and passwords

Adults and pupils 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. Adults will support pupils to do this.

Passwords for new users and replacement passwords for existing users can be allocated by the Network Technician or IT staff or DFR or ADFR for SIMS MIS system.

Adult users will change their passwords every 120 days, while pupils will change their passwords every year.

Training / Awareness

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

- Within the induction process at Torfield and Saxon Mount academy Trust.
- Through the school's e-safety policy and password security policy
- Through the Acceptable Use Agreement
- Through the schools GDPR policies relating to electronic security and communication

Students will be made aware of the school's password policy or given advice about password security:

- In ICT, PSHE or e-safety lessons.
- 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 such as IT support provider).

All users will be provided with a username and password by the Network support Technician who will keep an up to date record of users and their usernames.

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

- Prompts to change passwords will be provided every 90 days or 120 days dependent upon software.
- The password should be a minimum of 8 characters long and:
  Should include a minimum of three of the following: 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 to the ICT Coordinator, or the Network Manager (or other person). With Office 365 incorrect password input will automatically lock an account and a notification will be forwarded to an administrator to reset.

Audit / Monitoring / Reporting / Review

The responsible person (Assistant Head and /or DFR/ADFR) and the Network Technicians 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.

IT support provider senior staff and in exceptional circumstances, school senior leaders 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 IT Technician and IT managed service provider 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.

Staff found to be not working in compliance with this policy, resulting in data security breaches or compromising the schools network may be subject to disciplinary action.

Reviewed: October 2022

Next review: October 2023