THE SCHOOL PASSWORD PROTECTION POLICY

Updated on January 2021

Reviewed and approved by:

OSG TEAM

AL AMEER ENGLISH SCHOOL, AJMAN

PASSWORD PROTECTION CONTRACT 2020-2021

Introduction:

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities.

A safe and secure 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
- 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 Vice Principal
- Passwords for new users will be allocated by the ICT technician
- All users 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 and must immediately report any suspicion or evidence that there has been a breach of security
- Users will change their passwords at regular intervals

Staff Passwords :

- All staff users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames
- The password should be changed at regular intervals
- The password must not include proper names or any other personal information about the user that might be known by others
- Passwords shall not be displayed on screen
- Passwords should be different for different accounts, to ensure that other systems are not put at risk
- Passwords should be different for systems used inside and outside of school
- Password on Pupil Tracker should be changed regularly after 90 days by the user
- Teachers will be provided with a username and password to use ‘YouTube’ for teaching and learning purposes
- Teachers will be provided with a password to use the school website for uploading information on the school website

Pupil Login :

- Classes will be provided with a username by the ICT technician who will keep an up to date record of users
- Individual pupils will not be given an individual username and password
- Pupils will be taught the importance of password security
- Pupil Password should be changed regularly after 180 days for Grades KG1 to 7th and after 60 days for Grades 8th to 12th by the user

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 online safety policy and password policy
- through the Acceptable Use Agreement

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

- in lessons

Audit/Monitoring/Reporting/Review

The ICT technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Policy compiled by: Mrs. SELMA MOHAMMED

Reviewed on: September 2020

Next review date: March 2021

SCHOOL PASSWORD SECURITY POLICY 2020 - 2021

Suggestions For Use :

Securing sensitive data is becoming more and more difficult with users having access to so many devices, Wi-Fi and internet connectivity. Single Sign on and shared accounts means a security leak on one system could allow unauthorized access to others. Teachers and pupils have access to data, documents and systems from home, the school network via Wi-Fi from the school grounds and with cloud email and storage a lost password could give malicious users easy access to a host of systems.

Staff and students often don't realize the potential risks this poses and it is important that e-Safety training and guidance helps to educate both groups of users.

Tablets, iPads, mobile phones, cameras and home laptops often don't support good practice with required passwords and it is important that schools also consider the types of data held on these devices, particularly if leaving the school.

Schools should provide a safe and secure username and password system. This policy template has been written to provide guidance on how schools may wish to develop their own policy.

Introduction:

The school will be responsible for ensuring that the *school data and network* is as safe and secure as is reasonably possible and that:

- users can only access systems and data to which they have right of access
- users should agree to an acceptable use policy
- users should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- users must not store their passwords in plain view and staff must not write down passwords.
- access to personal data is securely controlled in line with the school's personal data policy
- where possible 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 IT systems, including email and Virtual Learning Environment (VLE).

Responsibilities :

All users provided with their own user accounts will have responsibility for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately change their password and report any suspicion or evidence that there has been a breach of security. Class accounts used for foundation pupils should be monitored by the class teacher and pupils should only use under supervision.

New user accounts, and passwords for existing users will be allocated by the IT Incharge.

Implementation :

Staff and pupil accounts must be disabled on leaving the school and user data deleted after 3 Months. School office staff should ensure that the ICT helpdesk is aware of the leavers as soon as possible.

All users must change their passwords occasionally to ensure systems remain secure. However the length between changes needs to take into account the type of user and the risk to the school if unauthorized access was gained. Similarly the complexity of password needs to reflect the user.

Users should change passwords to the following schedule and complexity

- Staff passwords every 90 days : Minimum 8 characters (Access only for the staff)
- Grade KG1 to Grade 7th every 180 days : Minimum 8 characters (Access only for the Parents)
- Grade 8th to Grade 12th pupil every 60 days : Minimum 8 characters (Access to Parents or Students)
- Foundation pupils class account every 365 days

Passwords should be of 8 characters which include 3 of the following types (upper, lower, numeric and special)

Passwords should not be re-used for 10 consecutive password changes.

Tablets or other devices syncing to email, cloud storage or storing data not able to meet these requirements must as a minimum use 4 digit pin codes with a lifespan of 60 days for staff or 365 days for pupils. The mail administrator may enforce stricter requirements.

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).

All users (KG and above) will be provided with a username and password. Users will be required to change their password at set intervals. Class log-ons for foundation pupils may be used but the school needs to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.

The following rules apply to the use of passwords:

- *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 (use of one-way encryption)*
- *Requests for password reset for a pupil should be requested by a member of staff. Password reset for a staff accounts must be requested by the individual directly.*

Where sensitive data is in use – particularly when accessed on laptops – schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

Audit / Monitoring / Reporting / Review :

The Password Security incharge will ensure that full records are kept of:

- *User Ids and enabled accounts*
- *Security incidents related to this policy*
- *Password Changes and Complaints*

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

(In Maintained schools) Local Authority Auditors 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 ... *(E-Safety Officer / E-Safety Committee / E-Safety Head/ Data Protection Officer (DPO))* at regular intervals *annually*.

This policy will be regularly reviewed annually in response to changes in guidance and security incidents.

Training / Awareness :

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorized access / data loss. This should apply to even the youngest of users, even if class logons are being used.

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

- at introduction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement Policy

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

- in ICT and / or e-safety lessons (the school should describe how this will take place) through the Acceptable Use Agreement

Evaluation :

This policy will be reviewed as part of the school's review cycle or if guidelines change

Students Online Acceptable Use Agreement

***AL AMEER* regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies.**

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

1. I will be a responsible user and stay safe when using the internet and other digital technology at school.
2. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
3. I will only use the school's internet and any device I may be using in school for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or after school.
4. I understand that all internet and device use in school may be subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used as if I am in school.
5. I will keep my logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it.
6. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
7. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
8. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
9. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
10. I understand that cyber bullying is unacceptable, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside.
11. I will not browse, download, upload, post or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
12. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions and I should respect this.
13. I will only e-mail or contact people as part of learning activities.
14. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
15. When using the internet, I will not download copyright-protected material (text, music, video etc.)
16. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

17. Live streaming can be fun but I always check my privacy settings and if I rarely (or preferably never) do anything that everyone on the internet can see. If I live stream, I tell a trusted adult about it.
18. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
19. I will only use my personal devices (mobile phones, USB devices etc) in school if I have been given permission to do so.
20. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
21. I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
22. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
23. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, I will not respond to it but I will save it and talk to a trusted adult.
24. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
25. I know who my trusted adults are at school, home and elsewhere, but if I feel I can't talk to them, I know I can call Childline or click CEOP.

I have read and understand these rules and agree to them.

Student name: _____

Signed: **_____** ***Date :*** **_____**