Schools and Community ICT Service
01970 633678
Ceredigion

Schools and Community ICT Service
01970 633678
Ceredigion

School Password Security Policy Template

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 unauthorised 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 realise 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 ICT 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 replacement passwords for existing users will be allocated by the ICT service desk or school technician.

Staff and pupil accounts must be disabled on leaving the school and user data deleted after 3 years. 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 unauthorised 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 chars including 3 of the following types (upper, lower, numeric, special)
- KS3 & 4 pupils every 180 days
  - Minimum 8 chars including 3 of the following types (upper, lower, numeric, special)
- KS2 pupils every 365 days
  - Minimum 6 chars
- Foundation pupils class account every 365 days

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 90 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 (at KS2 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 and the AUP. 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.

Schools must ensure that more than one person knows the administrator accounts for systems and where necessary a copy stored in the school safe.

Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records are kept of:

- User Ids and enabled accounts
- 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.

(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 Governor)* 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 unauthorised 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 induction
- 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