PASSWORDS POLICY

Rationale

- The purpose of this policy is to set out and communicate the Department of Education and Training's (the Department's) rules concerning the use and security of passwords that must be observed while conducting Departmental business, teaching and learning activities.
- The requirements defined within this policy will assist to mitigate the risk of unauthorised access to the Department's Information and Communications Technology (ICT) systems and applications, thereby safeguarding the confidentiality, integrity and availability of information essential to the needs of the Department.
- This policy applies to all Department ICT systems and applications that support Departmental services and which use the combination of a userID and a password for authentication, including but not limited to:
  - Systems and applications that have been developed by the Department.
  - Systems and applications that have been acquired by the Department.
  - Systems and applications that have been developed by an external party at the request of the Department.
  - Systems and applications owned by the Department but hosted at a third party data centre.
  - All environments.
- All users of the Department's ICT systems and applications including staff, teachers, contractors and any other individuals and organisations who have been granted access are covered by this policy.
- Exclusions:
  - Environments dedicated to ICT development activities that have been granted exclusion in writing from the Department's Executive Director, Information Technology Division (ITD) or delegate.
  - ICT systems and applications accessed by students other than eduSTAR.
  - Existing ICT systems and applications that cannot comply for technical or business reasons. However, the system or application owner must formally endorse the exception in consideration of the risks, and the exception must be approved by the Executive Director.

Purpose

- To ensure Footscray North Primary School is aware of and complies with DET's administrative requirements in regard to rules concerning the use and security of passwords within the school.
- To ensure the creation, management and protection of passwords used to access the Department's ICT systems and applications complies with DET guidelines and policy.
- To maintain the security and integrity of computer equipment at the school.

Definitions

Term	Definition
Administrator account	A userID with elevated access control privileges to an ICT application or system; not used for routine business purposes such as accessing the Department's email and login to the Department's network.
DET	The Department of Education and Training (the Department).
ICT systems and applications	Includes but not limited to all Department networks, systems and software including Department Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, Department email systems, computer systems, software and servers.
ICT	Information Communications & Technology
Initial password	A temporary password assigned to the userID on creation; user to change password at first login.
ISI PCB	Information Strategy Implementation Program Control

	Board.
ITD	Information Technology Division
Reset (temporary) password	A Password reset is an operation that allows an administrator or helpdesk operator to set another user's passwords to a desired new value.
School account	A userID and password allocated to a school primarily for the purpose of email communications with external parties including parents and organisations.
Service account	A userID and password allocated to an ICT system or application; not to a person. For example, an application is allocated a service account to access a backend database.
User	A person whom this policy applies to.
User account	A userID and password allocated to a person

Implementation

- Users are accountable for the actions performed when their userID and password are used to access Department ICT systems and applications.
- System administrators who are responsible for setting password controls must ensure that the controls comply with this policy.
- Personnel involved in application development or acquisition must ensure that the required password controls exist and can be configured to comply with this policy.
- Staff, students and other authorised users will take all reasonable steps to protect the secrecy of their passwords, including but not limited to the following:
  - Users must not share their userID and password with a third party.
  - Users must not write down their password and leave in a place where it could be easily found.
  - Users must take care when typing their passwords if they are being observed.
  - Users must change their password if they suspect that someone else knows it.
  - Users must not use their DET password as the password for any non-DET system.
- The Department's ICT systems and applications that authenticate users via a userID and password must comply with the following:
  - The password controls prescribed by this policy.
  - System administrators must change default vendor and manufacturer passwords during product installation.
  - Users must change their initial password at first logon.
  - The clear text password is not visible on the screen when entered by the user, except on mobile devices that briefly display each password character as it is entered.
  - Users must enter new passwords twice for confirmation of accuracy.
  - System administrators must ensure audit logs are kept of all password changes.
- System generated initial passwords and reset (temporary) passwords must be pseudo-random and comply with password construction rules prescribed in this policy.
- The following password controls apply to accounts assigned to individual users:

Policy Rule	Default	Staff with Employee ID	Students	Parents and Carers	Casual Staff Without Employee ID; School Visitors
Minimum password length	7	√	√	√	√
Maximum Password length	32	√	√	√	√
Password must be complex	Yes	√	√	√	√
Time period a user must keep a new password before changing it	1 day	√	√	√	√

Time period a password can be used before it must be changed	126 days	√	365 days	365 days	√
User receives a warning message before password expires	Yes	Via email, 14 days before	Via screen, 30 days before	Via screen, 30 days before	Via email to Administrator, 30 days before
When old password can be reused	After 8 new passwords	√	√	√	√
When an initial password expires if not used	After 30 days	√	√	√	√
When a reset (temporary) password expires if not used	After 10 days	√	√	√	√
When a screensaver activates after a defined period of user inactivity	After 15 minutes	√	√	√	√
Number of consecutive failed login attempts for the account to become locked	10 attempts	√	25 attempts	√	√
Number of minutes a locked account remains locked before it is unlocked automatically	30 minutes	√	√	√	√

√ indicates that a default rule applies

- The password must have a complex structure and contain at least one character from at least three of the four sets below.
  - Lowercase characters (a-z); Upper case characters (A-Z); Numeric characters (0-9);
  - Special characters and punctuation (e.g. !@#$%^&).

This policy prescribes password controls for students when accessing an enterprise application.

- The following password controls will apply to school accounts, administrator accounts, and service accounts.

Policy Rule	Default	School Accounts	Administrator Accounts	Service Accounts
Minimum password length	7	√	12	12
Maximum Password length	32	√	√	√
Password must be complex	Yes	√	√	√
Time period a user must keep a new password before changing it	1 day	√	√	Not set
Time period a password can be used before it must be changed	126 days	365 days	√	365 days
User receives a warning message before password expires	Yes	Via email to account and principal, 14 days before	Via email, 14 days before	Not set
When old password can be reused	After 8 new passwords	√	√	√
When an initial password expires	After 30 days	√	√	Not set

if not used				
When a reset (temporary) password expires if not used	After 10 days	√	√	Not set
When a screensaver activates after a defined period of user inactivity	After 15 minutes	√	√	Not set
Number of consecutive failed login attempts for the account to become locked	10 attempts	√	√	Not set
Number of minutes a locked account remains locked before it is unlocked automatically	30 minutes	√	√	√

√ indicates that a default rule applies

- The password must have a complex structure and contain at least one character from at least three of the four sets below.
  - Lowercase characters (a-z); Upper case characters (A-Z); Numeric characters (0-9);
  - Special characters and punctuation (e.g. !@#$%^&).

Please Note:

- A Service Account is one assigned to an ICT application or system, not to a person.
- A School Account is unique to a school and advertised to the public for the purpose of correspondence.
- A new password must be kept for at least 24 hours before being replaced.
- Staff will be briefed at least once per semester on the rules governing their use of ICT equipment at the school.
- New staff will be briefed as part of the induction process.
- For further information regarding this policy and the dispensation process, the College will contact The Manager, Risk Management & Compliance, via the online Service Gateway (https://www.eduweb.vic.gov.au/servicedesk/).

Evaluation

- This policy will be reviewed as part of the school's review cycle or if guidelines change (latest DET update November 2017).

This policy was ratified by School Council 25/3/2019

Reference:
Password Policy No. ICT PAG/1504
Published by ICT Division, Effective November 2015
www.education.vic.gov.au/eduPass/Pages/PasswordPolicy.aspx