Topic:	**Electronic Password Procedure for Email / Computer Logins**
Effective:	**February 2013**
Cross-Reference:	*Municipal Freedom of Information & Protection of Personal Privacy Legislation* *Halton District School Board Privacy and Information Policy* *Related Halton District School Board procedures (including but not limited to):* *Information Communications Technology Acceptable Use Procedure* *Protection of Board-owned Mobile Devices* *Board-assigned Mobile Devices*
Revision Date:	**February 2018**
Responsibility:	**Superintendent of Education – Information Services**

INTENDED PURPOSE:
The Halton District School Board will use an enforceable password process to provide greater complexity, proportional to the level of confidential and private electronic information for student or employee group(s) access.

PROCEDURES:
For the purposes of this Procedure, the following terminology and understanding will be applied.

1. Active Directory is the technology used to authenticate users logging in to their workstation and accessing network resources.

In developing these procedures, the following factors were considered:
a) Forced password changes – how frequently the user MUST change their password
b) Password history dictates if a formerly used password can be reused.
c) Complexity – the combination of numbers, upper and lowercase letters, punctuation.
d) Number of failed logins before the user is penalized. Penalties typically include a wait period before the user can successfully log in.

Each employee role will be assigned the "Password Level" found in the following table.

Employee Role	Password Level
Students	Basic
All school-based teaching staff	Regular
All Superintendents / Director	High confidentiality
All IT staff (regular accounts)	High confidentiality
IT staff (privileged accounts)	High security
School Operations Executive Assistants	High confidentiality
Communications Department, Director's Office Staff	High confidentiality
Student Services, Business Services, Human Resources	High confidentiality
Planning Department	Medium confidentiality
School Programs staff	Regular
Facility Services staff	Regular
School Administration (Principals, Vice-Principals)	High confidentiality
School Secretaries	High confidentiality
All other staff, including occasional staff	Regular
Trustees	Medium confidentiality

The following password change criteria will be applied to these employee groupings as per assigned security levels.

	Computer Login / Active Directory	Email Login	
Security Level	**Forced Password Changes**	**Password History**	**Forced Password Changes**
Basic	None (password can not be changed)	N/A	None
Regular	None (change when email [DM1]password changes)	Can re-use	12 months
Medium Confidentiality	90 days	Cannot use the last three (3) passwords	90 days
High Confidentiality	60 days	Reuse disabled	60 days
High Security	30 days	Reuse disabled	30 days *
			** A possession-based security solution is being evaluated*

All password changes will adhere to the following standards:

a) A password must contain a minimum of eight characters;
b) Active Directory: after eight (8) failed password attempts, an imposed wait-time of six (6) minutes occurs before a user can attempt to log in;
c) Password complexity requires three combinations of:
   i. lowercase letters
   ii. uppercase letters
   iii. symbols
   iv. numbers