Tower Hill Primary School
Password Policy

Date: September 2018 **Author: Laura Ovenden, DHT & DPO**
Review Date: September 2020

Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Tower Hill School's entire network. As such, all employees with access to Tower Hill's systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose
The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Main Objective
To ensure that all passwords in use by Tower Hill staff, or authorised contractors working for Tower Hill School shall meet the required criteria

Scope
This is applicable to ALL computing systems owned by Tower Hill School. It applies to all permanent and temporary employees and should be incorporated into contracts with third parties. All passwords shall conform to the following requirements in all case. This policy shall cover all assets that contain either Staff or pupil data.

Policy

Password Requirements (except Handheld Devices see Section 3.3)

- Passwords should be unique for each system used.
- Must not contain all or part of the user's account name
- Must be a minimum of six characters in length

Contain characters from two of the following three categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9) or Non-alphabetic characters (for example, !, $, #, %)
- Not be a simple dictionary word
- Not be readily guessable – eg phone number, pet's name, car type, date of birth
- Must not contain proper names, of people, companies, products etc
- Must not be a word in any language, slang, dialect, jargon, etc.
- Must not contain adjacent, consecutive or repeated letters or numbers

*A useful technique for password maintenance for each different system is to have the same word/number password e.g. Merlot11, and add a letter into the word at a specific location (e.g. 4th letter) that changes for each system – using the first letter of the name of that system.

e.g. for www.outlook.com: MerOlot11, for www.Autotrader.com: MerAlot11, for www.eschools.co.uk: MerElot11

Password Use and Maintenance

All users shall change their passwords at least once per term. On systems where this is technically possible, the user shall be reminded when the password must be changed.

Passwords not assigned by the user (i.e. assigned by Harrap or other IT providers) shall be regarded as temporary and must be changed on the first login. This change is automatically enforced on systems where this is technically possible.

After six unsuccessful login attempts the user shall be locked out. If this happens, the user shall contact Harrap to request assistance·

It is recommended that members of staff do not use the "Remember Password" feature of applications. Going against this recommendation is done at the users own risk.

All passwords must be kept strictly confidential, and not written down or otherwise recorded in a way (including any computer system (including iPad's or similar devices)) which means they could be learned by others. They must not be shared with other personnel. If a password is considered to be compromised, it must be reported as a security incident and changed immediately.

Handheld Devices (e.g. iPads)

The restrictions function will be password protected by the ICT Co-ordinator using a 4 digit number known only by that person.