Greenholm Primary
Greenholm Road
Great Barr
Birmingham
B44 8HS
0121 464 6321

Password Management Policy

Document Owner	: Greenholm Primary School ICT Dept.
Version	: 1.0
Date	: December 2013

Greenholm Primary School
"working together for the good of all our children"

Table of Contents

Overarching statement

At Greenholm we are a school that is welcoming, safe and creates an environment which values and supports everyone learning. We work hard to create an ethos that promotes inclusive practice for all, by providing a consistent and fair approach, which is supportive of the continual emotional development of all and by demonstrating mutual respect, openness and honesty.

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this policy is to establish standards for the creation of effective user level passwords, the protection of those passwords, and the mechanism and frequency of password change.

1.2 Background

1.2.1 Passwords are used for various purposes. Some of the more common uses include: user level accounts, application accounts, web accounts and screen saver protection. Everyone must be aware of how to select suitable passwords.

1.2.2 Passwords are an important aspect of computer security. They are the frontline of protection for user accounts. A user who carelessly selects a password may compromise an entire network.

1.2.3 Poor password management can result in security breaches and have serious implications including:

- Loss of reputation & credibility;
- Loss of clients and public trust;
- Loss of data and information;
- Financial loss (remedial work, penalties, direct loss, consequential loss);
- Criminal or civil action.

1.3 Scope

1.3.1 This policy applies to the use of passwords on ICT facilities for which the School operates or is accountable and responsible. It is applicable to both School staff and pupils.

1.4 Linked/Other useful policies/procedures

1.4.1 This policy should be read in conjunction with the:

- Acceptable Use of ICT Policy (Schools).

2 RESPONSIBILITIES

2.1 School

2.1.1 **Induction, Training and Support –** The School is responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy.

2.1.2 **Awareness Training –** The School will provide awareness training to pupils in the management of passwords.

2.1.3 **User Access –** The School is responsible for ensuring the staff and pupils they have approved and authorised to access the School Network and ICT resources are aware of and comply with this policy.

2.2 Staff

2.2.1 **Training** - All staff should attend the appropriate training course.

2.2.2 **Breach of this Policy** - Staff found to be in breach of this policy may be disciplined in accordance with the *Schools Disciplinary Policies and Procedures*. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

2.3 Pupils

2.3.1 **Awareness Training** - Pupils should attend the appropriate awareness training.

2.3.2 **Breach of this Policy** - Pupils found to be in breach of this policy may be disciplined in accordance with the *Schools Disciplinary Policies and Procedures*.

3 PASSWORDS

3.1 Staff Passwords

3.1.1 **User Name and Password** - All staff must have a unique user name and password.

3.1.2 **Format of Password (Staff)** - All user-level passwords (e.g. for desktop computers, line-of-business applications) must as a minimum:

- be at least eight characters long;
- not contain your user name, real name, or company name;
- not contain a complete dictionary word;
- be significantly different from previous passwords (not Password1, Password2, Password3…etc);
- contain characters from three of each of the following four groups:

Group	Examples
Uppercase letters	A, B, C …
Lowercase letters	a, b, c …
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : “ ; ‘ < > ? , . /

3.1.3 **Remembering Passwords** - To assist staff in remembering passwords they may take a standard word or phrase and substitute the consonants or vowels with upper and lower case letters, numerals and symbols:

- “chronicle” becomes “c#r0n1cLe”
- “happy-hour” becomes “#A99y_#0uR”

3.1.4 **Security of Passwords** - Staff may keep a record of their password provided it is kept locked securely.

3.1.5 **Password Changes** - All user-level passwords must be changed every 42 days. Staff will be prompted to change the password prior to this. Staff will not be allowed to repeat the use of a password sooner than 5 changes.

3.1.6 **Password Lock Out** - Staff will be locked out of their systems if they have 5 successive login failures. Staff locked out should contact their *Schools ICT Support* for assistance however password attempts reset after 30mins.

3.1.7 **Staff must <u>not</u>:**

- share passwords with anyone, including other members of staff, pupils, ICT support staff, friends or family members;
- insert passwords into email messages or other forms of text based electronic communication;
- log on to a machine using their password for another individual to then use.

3.1.8 **Shared User Accounts** - Staff should not use applications that have shared user accounts and passwords unless specifically approved to do so by the SMT or ICT staff.

3.1.9 **‘Remember Password’ Feature** - Staff should not use the ’Remember Password’ feature of some applications, e.g. when accessing websites.

3.1.10 **Compromised User Accounts or Passwords** - If a member of staff believes that a user account or password has been compromised, this should be reported to their *Schools ICT Support* and all passwords must be changed.

3.2 Pupil Passwords

3.2.1 **User Name and Password** - All pupils must have a unique user name and password where one is necessary.

3.2.2 **Format of Password (Pupils)** - All user-level passwords (e.g. for desktop computers, line-of-business applications) must as a minimum:

- be at least six characters long;
- contain characters from two of each of the following four groups:

Group	Examples
Uppercase letters	A, B, C …
Lowercase letters	a, b, c …
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : “ ; ‘ < > ? , . /

3.2.3 **Remembering Passwords -** To assist pupils in remembering passwords they may use a word including an uppercase letter and followed by a numeric e.g. White2, Blue10, Windy1.

3.2.4 **Security of Passwords** - Pupils may keep a record of their password provided it is kept securely.

3.2.5 **Password Changes** - All pupil user-level passwords must be changed at least annually (Autumn Term).

3.2.6 **Password Lock Out** – Pupils will be locked out of their systems if they have 5 successive login failures. Pupils locked out should contact their Teacher or *Schools ICT Support* for assistance however password attempted reset after 30mins.

3.2.7 **Pupils must <u>not</u>:**

- share passwords with anyone, including other pupils, teachers, ICT support staff, friends or family members;
- insert passwords into email messages or other forms of text based electronic communication;
- log on to a machine using their password for another individual to then use.

3.2.8 **Shared User Accounts** - Pupils should not use applications that have shared user accounts and passwords.

3.2.9 **‘Remember Password’ Feature** – Pupils should not use the ’Remember Password’ feature of some applications, e.g. when accessing websites.

3.2.10 **Compromised User Accounts or Passwords** - If a pupil believes that a user account or password has been compromised, this should be reported to their teacher or *Schools ICT Support* and all passwords must be changed.

4 FURTHER ADVICE

For further advice on this policy, please contact:

***Schools ICT Support*, Senior Management Team**

5 GOVERNANCE

This policy is to be used to relation with other applicable policies where appropriate and not in lieu of.

6 DOCUMENT CONTROL

Changes History

Version	Date	Amended By	Change
1.0	December 2013	Daniel Hunt	Initial Creation
1.1	January 2015	DH	Updated for Overarching Statement
1.2			

Approval

Role	Name	Signed	Date
Policy & Compliance Manager	G Turner		December 2013