LITTLE PLUMSTEAD CE VA PRIMARY SCHOOL

PASSWORD SECURITY POLICY

This policy is based on the password security guidance given by the National Cyber Security Centre (NCSC), part of GCHQ in November 2018.

In addition the Information Commissioner's Office (ICO) advises schools to take the security of personal data very seriously. The loss of, or unauthorised access to, personal data could prompt legal action or cause the ICO to impose financial penalties.

The Headteacher has overall responsibility for the school's ICT security.

Introduction: the problems with passwords

NCSC advises that the death of the password was predicted some ten years ago. It was assumed that alternative authentication methods would be adopted to control access to IT infrastructure, data, and user material. But since then, password use has only risen.

This increase in password use is mostly due to the surge of online services. Passwords are an easily-implemented, low-cost security measure. However, this proliferation of password use, and increasingly complex password requirements, places an unrealistic demand on most users.

Inevitably, users will devise their own coping mechanisms to cope with 'password overload'. This includes writing down passwords, re-using the same password across different systems, or using simple and predictable password creation strategies. A study within a Scottish NHS trust found that 63% of its users admitted to re-using passwords.

How are passwords discovered?

The NCSC has identified that attackers use a variety of techniques to discover passwords. Many of these techniques are freely available and documented on the Internet, and use powerful, automated tools.

Approaches to discovering passwords include:

- social engineering eg phishing; coercion
- manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names
- intercepting a password as it is transmitted over a network
- 'shoulder surfing', observing someone typing in their password at their desk
- installing a keylogger to intercept passwords when they are entered into a device
- searching an enterprise's IT infrastructure for electronically stored password information
- brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found
- finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device
- compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords.

Change all default passwords

Default passwords being left unchanged is one of the most common password mistakes that organisations make. By leaving default credentials in place, networking and crucial infrastructure is reachable online. In 2012, the 'Carna Internet Census' found "several hundred thousand unprotected devices on the Internet". The Carna botnet commandeered these devices with default passwords to create a temporary research botnet.

All default passwords that come with any system or software should be changed before deployment by the school's ICT Technician. Any default or automatically generated passwords set by ICT Shared

Services or the school's ICT Technician when setting up a new user or device should be changed by the user when first logging on to the device/email.

The school's ICT Technician will carry out regular checks of the system devices and software specifically to look for unchanged default passwords.

Help users cope with password overload
Users are generally told to remember passwords, and to not share them, re-use them, or write them down. However the school recognises that the typical user has dozens of passwords to remember.

The school will only implement passwords when they are really needed as a way to minimise the password burden. Systems and services with no security requirements should be free from password control.

Changing passwords
The school recognises that some systems will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user (who is likely to choose new passwords that are only minor variations of the old) and carries no real benefits as stolen passwords are generally exploited immediately. The school believes that long-term illicit use of compromised passwords is better combated by:

- staff setting complex passwords (see below)
- monitoring logins to detect unusual use
- notifying users with details of attempted logins, successful or unsuccessful; they should report any for which they were not responsible.

NCSC advises that regular password changing harms rather than improves security. However, users must change their passwords on indication or suspicion of compromise.

Sharing passwords
The school does not allow password sharing between staff users and between pupil users. Sharing accounts, or even occasional use by anyone other than the account holder, negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost. However in order to support the pupils, individual teachers have access to their class pupils' email passwords.

Setting a strong complex password
In accordance with the ICO advice, passwords used by staff should:

- Be long
- Include a range of characters, such as:
  - Upper case and lower case letters
  - Numbers
  - Punctuation marks
  - Other symbols
- Not contain dictionary words, where possible
- Not include simple substitutions of characters, e.g. "p4$$w0rd"
- Not include patterns derived from the keyboard layout, e.g. "qwerty"

Given the infeasibility of memorising multiple passwords, the school recognises that many are likely to be re-used. Users should only do this where the compromise of one password does not result in the compromise of more valuable data protected by the same password on a different system. Therefore school users should never use the same password for both home and school.

Reinforcement of this password policy will be undertaken through staff induction and training that helps users to avoid creating passwords that are easy-to-guess. The induction/training will advise that passwords should avoid personal information (names, dates, sports teams, etc.), simple dictionary words or predictable keyboard sequences.

School hardware and devices requiring password protection

School server
Teacher laptops
Teacher iPads
School Office desktop computers
Pupil laptops (although it is noted that pupil laptops are not used to store any data)

School software and important websites requiring password protection

Staff nsix email addresses
Pupil nsix email addresses
Generic school 365 mail email addresses
Pupil Asset
DfE Secure Access website
DfE NCA Tools website
Parentmail
Budget Planner
STAR Accounts
Staff Sickness Insurance
AnyComms +
HR Workspace
Barclays Bank
Tapestry
Norfolk Disclosure Service
Single Central Record

Summary of responsibilities

School's ICT Technician

- Create default passwords for new users and new devices.
- Carry out regular checks of the system devices and software specifically to look for unchanged default passwords.

ICT Shared Services, Norfolk County Council

- Monitor irregular, suspicious and failed login attempts.

School Office Manager

- Receive and securely store the nsix account email addresses and passwords of staff and pupils.
- Receive and securely store the Office 365 mail addresses and passwords.

Staff responsibilities

- Replace a default or automatically generated password with a new password when provided with a new device when first logging on to the system/device.
- Set strong complex passwords as mentioned above, avoiding personal information (names, dates, sports teams, etc.), simple dictionary words or predictable keyboard sequences when creating passwords.
- Never re-use passwords between school and home.
- Share pupils' passwords only with the individual pupil, ensuring they keep it safe and reminding them not to share with others.

Pupil responsibilities

- To keep their passwords secure and not share with other

Drawn up by: School Office Manager using advice from NCSC and ICT Shared Services

Approved by governors: Spring 2019

Review date: Spring 2022